



جامعة مؤتة
عمادة الدراسات العليا

جريمة الاحتيال الإلكتروني دراسة تحليلية مقارنة

إعداد الطالب
حمزة عاطف علي المعايطة

إشراف
الأستاذ الدكتور عبد الإله النوايسة

رسالة مقدمة إلى عمادة الدراسات العليـــــا
استكمالاً لمتطلبات الحصول على درجـــــــة
الماجستير في الحقوق قسم القانون الخاص

جامعة مؤتة، 2012

الآراء الواردة في الرسالة الجامعية

لا تُعبِّر بالضرورة عن وجهة نظر جامعة مؤتة



بسم الله الرحمن الرحيم



MUTAH UNIVERSITY
Deanship of Graduate Studies

جامعة مؤتة
عمادة الدراسات العليا

نموذج رقم (14)

قرار إجازة رسالة جامعية

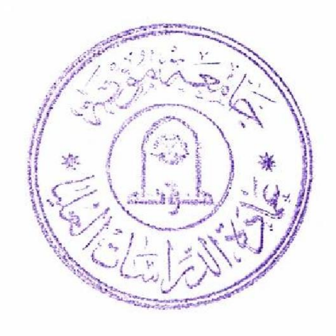
تقرر إجازة الرسالة المقدمة من الطالب حمزة عاطف المعايطة الموسومة بـــ:

جريمة الاحتيال الإلكتروني/ دراسة تحليلية مقارنة

استكمالاً لمتطلبات الحصول على درجة الماجستير في **القانون.**

القسم: القانون العام.

	التوقيع	التاريخ	
أ.د. عبدالاله محمد النوايسة		2012/04/26	مشرفاً ورئيسا
أ.د. نظام توفيق المجالي		2012/04/26	عضواً
د. مخلد ارخيص الطراونة		2012/04/26	عضواً
د. أكرم طراد الفايز		2012/04/26	عضواً



عميد الدراسات العليا
أ.د. عبدالفتاح خليفات

MUTAH-KARAK-JORDAN
Postal Code: 61710
TEL :03/2372380-99
Ext. 5328-5330
FAX:03/ 2375694
e-mail: dgs@mutah.edu.jo sedgs@mutah.edu.jo
http://www.mutah.edu.jo/gradest/derasat.htm

مؤته – الكرك – الاردن
الرمز البريدي: 61710
تلفون: 99-03/2372380
فرعي 5328-5330
فاكس 03/2 375694
البريد الالكتروني
الصفحة الالكترونية

الإهداء

إلى من تتناحر الكلمات لتخرج معبرة عن مكنون ذاتها

من تجرعت شقائي وعثراتي وعلمتني معنى الوفاء

أمُي الحبيبة ...

إلى كل من تورد بعلمه عقل غيره

وهدى بجوابه حيرة سائليه

فأظهر بوقاره تواضع العلماء

ونزل بقدره مُتكئاً لغيره

أساتذتي الكرام ...

إلى من غاب بريق عينها عن نبل كلماتي وأبا القلم أن يخط اسمها

إلى من تراقصت بها خيوط الظلام بعيداً...

لا تحزني فأنتِ اليوم هنا.....

إلى كل من جابت عيناه الدنيا

وشاح به نظره إلى هذا الجهد المتواضع

إلى هذا الصرح العلمي الفتي الجبار

جامعة مؤتة...

حمزة عاطف المعايطة

الشكر والتقدير

اللهم إني أسألك صحة في إيمان، وإيمان في حُ ُسن خلق، وصلاحاً يتبعه نجاحٌ وفلاح.

أتقدمبجزيل الشكر والامتنان والتقدير ، إلـــى أســتاذي الــدكتور عبدالالــه النوايسه، الذي علمني ووجهني كيف أتعايشبين صفحات الكتب ، لأنهل منها أفضل العلم، إضافة إلى عنائه وسهره في القراءة والإشرافعلى هذه الرسالة ، ومتــابعتي الحثيثة لحين انجازها، فجزاه الله خير جزاء.

كما أتقدمبوافر الشكر والتقدير ، إلى الأساتذة الأجلاء، أعضاء لجنة المناقشة الكرام، لما بذلوه من عناء قراءة هذه الرسالة، وتدقيقها وتصويبها لترى النور.

ولا أنسى أنتقدَّم بجزيل الشكر والعرفان ، إلى كل من مد لي يــد العــون وساعدني وقدم لي كافة المعلومات الغنية في كتابة رسالتي.

وآخر دعوانا أن الحمد لله رب العالمين

حمزة عاطف المعايطة

الصفحة	فهرس المحتويات

فهرس المحتويات	الصفحة
1.1.2 الاحتيال الإلكتروني من خلال أنظمة الحوالات البنكية الإلكترونية...................................	70
2.1.2 رسائل البريد الإلكتروني الخادعة..................	73
2.2 جرائم الاحتيال الإلكتروني بواسطة بطاقات الدفع الإلكتروني.	80
1.2.2 نشأة وتطور بطاقات الدفع الإلكتروني.............	80
2.2.2 أطراف العملية التجارية لبطاقات الدفع الإلكتروني وأنواعها..	83
3.2.2 أهم أنماط الاعتداء على بطاقات الائتمان..........	87
3.2 كيفية مواجهة جرائم بطاقات الدفع الإلكتروني................	92
1.3.2 المواجهة التشريعية لجرائم بطاقات الدفع الإلكتروني	92
2.3.2 الحلول الفنية المساهمة في مواجهة جرائم بطاقات الدفع الإلكتروني....................................	95
3.3.2 الجهود الدولية في مكافحة جرائم الاحتيال الإلكتروني	101
4.2 المواجهة التشريعية لجرائم الاحتيال الإلكتروني في التشريع الأردني..	107
1.4.2 المواجهة التشريعية لجرائم الاحتيال الإلكتروني في قانون العقوبات....................................	108
2.4.2 مدى مواجهة قانون المعاملات الإلكترونية وقانون جرائم أنظمة المعلومات لجرائم الاحتيال الإلكتروني.	114
3.4.2 دور الأجهزة الأمنية والجهات المتخصصة في الحد جرائم الاحتيال الإلكتروني في الأردن...............	123
5.2 الخاتمة..	126
المراجع...	130

قائمة الجداول

الملخص

جريمة الاحتيال الإلكتروني دراسة تحليلية مقارنة

حمزة عاطف علي المعايطة

جامعة مؤتة، 2012

إنَ عجلةَ التقدم العلمي وتكنولوجيا المعلومات ، ألقت بظلالها على منظومة الحياة اليومية في كثير من المجالات الاقتصادية ، والاجتماعية، والأمنية، وأنْ أيّ نتاج تقدمي جديات لا يخلو من المخاطر ، والتحديات المرافقة عند استعماله بشكل غير شرعي ومحاولة تغيير المفاهيم عن حقيقتها ، وعلى رأسها جرائم الاحتيال الإلكتروني فقد تناولت هذه الدراسة جريمة الاحتيال التقليدية ، وأركانها، والشروع فيها، لتمييزها عن جرائم الاحتيال الإلكتروني، كتمهيد من أجل التعريف بجرائم الاحتيال الإلكتروني وحجم هاوسمات مرتكبي هذه الجرائم ،ودوافع ا رتكابها، وأهم الإحصائيات الخاصة بهذه الجرائم ، والفئات المستهدفة بها، من ثم بيان أركان هذه الجريمة من الركن المادي ، والنتيجة الإجرامية المتحققة، والشروع فيها، والقصد الجرمي للجريمة.

كما تناولت الدراسة أهم صور وأساليب هذه الجرائم، بالإضافة إلى دور الأجهزة الأمنية في الأردن، في الحدّ من هذه الجرائم،وبينت الدراسة المنهج التشريعي الأردني لهذه الجرائم، والتشريعات والعربية والأجنبية.

واستعرضت الدراسة الجهود الدولية المبذولة في مكافحة هذه الجرائم والحد من آثارها.



Abstract

Electronic Fraud Crime: Analytic and Comparative Study

Hamzah Atif Al-Ma'aytah
Mu’tah University, 2012

Scientific progress and information technology (IT) have affected daily life system in many social, economic, and security dimensions, and any new progressive product isn't far away from the associated risks and challenges when using it illegally, and attempting to turnover and change the concepts from their real meanings. The major topic in this matter is electronic fraud crimes. The current study addressed the traditional fraud crime, its aspects, and the athempl to committ it as an introduction to identify this traditional Crime from the electronic fraud crimes through disclosing its range feature of outspends and electronic fraud crimes, the range of it, characteristics of offenders, and the motives to commit such crimes. The study also aimed at highlighting the most important static's regarding this crime and the subjected categories, and to clarify and explain its aspects and components such as the material component the resulted criminal consequence, committing it, and the criminal intent which is represented by the cognitive component of the crime. The study also addressed the most important forms and methods of electronic fraud crimes, in addition to the Jordanian Security Departments' role in preventing these crimes. Also, it addressed legislative confrontation to these crimes in Jordanian, Arab, and foreign legislations, and reviewed the international efforts to present and compel these crimes against electronic fraud crimes.



المقدمة

من الضرورة بمكان تسليط الضوء بشيء من الإيضاح والتفصيل ، على ظاهرة جديدة تندرج ضمن باقة الجرائم الإلكترونية، ألا وهي جريمة الاحتيال الإلكتروني؛ لارتباط هذه الجريمة بتكنولوجيا المعلومات ، المتمثلة بالحاسبات الآلية وشبكة الانترنت التي تمثل البيئة الخصبة لها، فبات من الضرورة دراسة هذا النوع من الجرائم وخصائصها وأدواتها، والوقوف على التشريعات الناظمة لها، لما لهذا النوع من الجرائم من ارتباط وثيق في تقدم المجتمعات ، ومقدرتها على مواكبة العملية التكنولوجية المتقدمة في عصب الحياة الاقتصادية لأي بلد ، ورمز الانفتاح الاجتماعي التواصلي الذي أصبح مقياس لا يمكن تجاهله لقوة الدول ، من خلال توفير المناخ الآمن على مختلف الأصعدة[1].

أهمية الموضوع:

تتبلور أهمية دراسة هذا النوع من الجرائم ، من خلال جوانب كثيرة تعكس ضرورة الجدية في التعاطي معها من خلال الصعوبة في تكييف مثل هذه الجرائم وحداثتها المستمرة، وضرورة التدخل التشريعي لها، فأصبح الأمر يحتاج إلى جهدٍ في صقل التوعية القانونية لهذا النوع من الجرائم ، لذلك لابد من وقفة نضع فيها أهمية هذا البحث ، بما يتناسب وهذه الجرائم الإلكترونية، التي باتت من ضروريات الحياة على الصعيد الاقتصادي، المتمثل بالبنوك، والمؤسسات المالية ، ومجال التجارة الإلكترونية[2]، التي تضع العالم بين أيدي مستخدمي هذه التكنولوجيا العصرية، وعلى الصعيد الأمني الذي بات جل مرتكزاته ، ونطاق الحماية الدفاعية لديه تعتمد في المقام الأول على تكنولوجيا المعلومات، مع الإشارة إلى أنّه بات استخدام الحاسبات الآلية المتصلة بالانترنت تدق معظم الأوساط الاجتماعية ، وهو عنوان حاضر في نسق الحياة الخاصة للأفراد ، بتغطية أعمالهم ونشاطاتهم على

---

(1) عرب، يونس، (2002)، جرائم الكمبيوتر والانترنت، مؤتمر الأمن العربي للدراسات والبحوث الجنائية، أبو ظبي بالفترة الواقعة من 10 إلى 2002/2/12، ص3.

(2) المطيري، أنور بدر، (د.ت)، ظاهرة جرائم الكمبيوتر والانترنت، متوفر عبر الموقع: p1 of, 6, date 16/4/2011www.lawweb.cc/d1/d7.doc

الصعيد العلمي والترفيهي ، وممارستها من جميع الفئات العمرية وكلا الجنسين دون اعتبارها حِكراً على فئة أو مجموعة أشخاص بعينهم، فتثبت حينها الضرورة التشريعية التوعوية، لتحديد وإيضاح المخاطر المتولدة عن هذا الاستخدام غير المشروع، الذي يتولد عنه في المحصلة الجريمة المعاقبَ عليها[(1)].

مشكلة البحث:

هنالك تباين واضح، في القوانين الناظمة لموضوع الدراسة "الاحتيال الالكتروني" على الصعيدين العربي والأجنبي، وأبرزها تفاوت حجم هذه الثورة المعلوماتية، التي تمثل بيئة وأدوات هذه الجرائم، التي تميزها عن الجريمة التقليدية من بلد إلى آخر، مما يرتب عليه تتفاوت بين التشريعات من حيث التكييف، والعقوبة وآليات الردع القانونية، وبالتالي ضُعْف التعاون الدولي، وبما أن تكنولوجيا المعلومات وثورة الحاسب الآلي ، والانترنت، واعتماد المؤسسات المالية في القطاعين العام والخاص وآلية التعامل بها مترابطة مع بعضها البعض، على الصعيدين المحلي والعالمي، فإنه يشترك بها جميع الفئات التي من شأنها، ابتكار آليات جديدة من طرق الاحتيال الإلكتروني بشكل مختلف وواسع النطاق[(2)]، في حين نجد تدخل المشرع يحتاج إلى فترة زمنية طويلة، لأعداد نصوص تشريعية تحدد طبيعة هذه الجرائم وتقر العقوبات الرادعة لها ، من أجل الحفاظ على أوجه الاستقرار الأمني، والاقتصادي والاجتماعي، التي تصب في حفظ الحقوق العامة والخاصة للأفراد، التي تكفلت بها معظم الدساتير.

أما على الصعيد المحلي فإننا نجدُ قصوراً في التشريع الأردني الذي لم يخصص من النصوص العقابية، ما يكفي لسد النقص في كل من قانون المعاملات الإلكترونية المؤقت رقم (85) لسنة 2001، وقانون البنوك رقم (28) لسنة 2000، وقانون الأوراق المالية رقم (76) لعام 2002، وقانون العقوبات ومدى كفايتهم

---

(1) المكتبي، زاد، (2007)، تكنولوجيا المعلومات وتطبيقاتها في حياتنا، جريدة القدس، متوفر عبر الموقع: www.arablibrariannet.blogspot.com. p 1 of 1, date 13/10/2011

(2) منصور، محمد حسين، (2003)، المسؤولية الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، ص8.

للتصدي لمثل هذا النوع من الجرائم ، والتي باتت تشكل ظاهره تستحق المواجهة، وإن كان قانون جرائم أنظمة المعلومات المؤقت ، رقم (30) لسنة 2010، تناول مثل هذا النوع من الجرائم ، إلاّ أننا بحاجة إلى وجود نصوص أكثرَ تخصصاً من أجل استخدام أمثل لهذه التقنية، بالإضافة إلى حداثة هذا النوع من الجرائم ، وتطورها بحسب النسق التقدمي المرتبط بتكنولوجيا المعلومات ، وما يتمخض عنها من جهل الكثير من الفئات المستخدمة لها، والفهم الخاطئ للبعض بصعوبة اكتشاف مثل هذه الجرائم، والتي توفر لهم ، مرتعاً لخلق بيئة تقودهم بدورها إلى مواصلة ارتكاب هذه الجرائم، دون الوقوف على دراسات تمكنهم من تصحيح هذه المفاهيم المغلوطة ، وهذا ما نسعى إلى توضيحه من خلال هذه الدراسة.

نطاق البحث:

سوف نتناول في هذه الدراسة، مفهوم جرائم الاحتيال الإلكتروني وفق التشريع الأردني مقارنة مع التشريعات العربية والأجنبية، وأدواتها وخصائصها والمخاطر المتمخضة عنها، والآلية التشريعية في الحد من ارتكاب هذا النوع من الجرائم، بالإضافة إلى الموقف التشريعي الناظم لها، والاجتهادات الفقهية، والأحكام القضائية في مجال الاحتيال الإلكتروني، والإحصاءات المتعلقة بهذه الجرائم من الجهات الأمنية ذات الاختصاص ، والجهود الدولية في المعالجة والتصدي لمثل هذا النوع من مخاطر تكنولوجيا المعلومات ، مع بيان التفرقة في أركان وظروف هذا النوع من الجرائم، عنه في جريمة الاحتيال التقليدية كإحدى الجرائم الواقعة على الأموال.

بعض الدراسات السابقة:

لا توجد رسائل علمية لدرجة الماجستير ، أو الدكتوراه تحمل عنوان الاحتيال الإلكتروني أو المعلوماتي، على الصعيد المحلي والعربي بحسب علم الباحث ، إلا أنّه هنالك بعض الدراسات والمؤلفات، التي تناولت موضوع الاحتيال الإلكتروني ، بشكل جزئي غير متخصص ضمن المؤلفات المتخصصة، في الجرائم الإلكترونية والمعلوماتية ونذكر منها:

دراسة(قورة، 2005)جرائم الحاسب الآلي الاقتصادية ، حيث بين بعـــض صـــور جرائم الاحتيال الإلكتروني، وتعريفها، وأهم الوسائل المستخدمة في هذه الجـــرائم، بحكم أنها ضمن باقة الجرائم المندرجة تحت مظلة جرائم الحاسب الآلي، وســـوف يكون من المراجع الأساسية لهذه الدراسة

(دراسةالطوالبة، 2008)،الجرائم الإلكترونية ، والذي تناول به الجريمة الإلكترونية ككل، ولم يتناول جرائم الاحتيا ل الإلكتروني، إلا من خلال ذكر بعض وسائل هـــذه الجرائم، كونها تُصنف ضمن الجرائم الإلكترونية المستحدثة، وبالتالي وجبت الإشارة إليها.

(دراسةالمومني،2008)، الجرائم المعلوماتية ، حيث ركز هذا المؤلـــف، علـــى تحديد المفهوم القانوني للجرائم المعلوماتية، وما يميزها عـــن بـــاق ي الجـــرائم، وتناول بشكل موجز، بعض أنماط جرائم الاحتيال الإلكتروني، والتعريف الفقهي لهذه الجرائم؛ لارتباطها بالأنظمة المعلوماتية أساس هذه الجرائم.

(دراسة فوزي،2007)وعي المواطن العربي تجاه جرائم الاحتيال ، حيث تناول أحد صور جرائم الاحتيال الإلكتروني، مداراً للبحـــث وهـــو (بطاقـــات الـــدفع الإلكتروني نموذجاً) لهذه الجرائم في حين لم يتطرق إلى المفهوم القانوني لهـــذه الجرائم، ووسائلها، والكثير من صور جرائم الاحتيال الإلكتروني.

(دراسة الغثبر ؛ وابن هيشة، سليمان،2009)، الإصطياد الإلكتروني، حيث تنـــاول بعض صور وآليات الاحتيا ل الإلكتروني والوقاية منها، حيث ساد على هذا المؤلف، الطابع الاجتماعي الوقائي بعيداً عن الموقف القانوني من هذه الجرائم.

وتنفرد هذه الدراسة بتناولها عدداً من جرائم الاحتيال الإلكتروني، مع بيـــان أهم صور وأساليب هذه الجرائم، بشكل متخصص ومنفـــرد عـــن ســـابقاتها مـــن المؤلفات، من الناحية القانونية التحليلية والمقارنة، إضافة إلى أن جميع الدراســـات السابقة، لا سيما التي تعرضت للقانون الأردني، كانت سابقة على صـــدور قـــانون جرائم أنظمة المعلومات، لسنة 2010، وبالتالي فإن هذه الدراسة تنفـــرد بتناولهـــا جرائم الاحتيال الإلكتروني وفق هذا القانون.



منهجية البحث:

سوف نتناول دراسة هذا الموضوع وفقاً للمنًهج التحليلي ، (تحليل المحتـــوى) والمنهج المقارن (التشريع الأردني مع بعض التشريعات العربية و الأجنبية)، والذي يُمكن من خلاله التعرف على مضامين النصوص القانونية ذات العِلاقـــة، وبيـــان مراميها والوقوف على التطبيقات القضائية في هذا المجال.

تقسيم الدراسة: سوف نقسم الدراسة إلى فصلين: تناولت بالفـــصل الأول : التعريف بجرائم الاحتيال الإلكتروني وما يميزها عن جرائم الاحتيال التقليدية، مـــن خلال التعريف بمفهوم جرائم الاحتيال الإلكتروني وفق التشريع الأردني والتشريعات المقارنة، وحجمها وأركانها ووسائل هذه الجرائم المـــستحدثة، والـــصفات العامـــة لمرتكبي هذه الجرائم، وضحاياها المحتملين، في حين تم تخصيص **الفصلَ الثـــاني :** لأهم صور جرائم الاحتيال الإلكتروني، من خلال أجهزة الحاسب الآلي، وبطاقـــات الدفع الإلكتروني، ورسائل البريد الإلكترونـي الخادعة، وآلية الحد من ارتكاب هـــذه الجرائم من الناحية التشريعيـة، على الصعيدين المحلي والدولي، والجهـــود الدوليـــة المبذولة لمكافحة هذا النوع من الجرائم.



الفصل الأول

ماهية الاحتيال الإلكتروني

تمهيد وتقسيم:

يُعَدُّ اَلْاحتيالُ الْإلكتروني، من الجرائم المستحدثة ووليدة التطور التكنولوجي والثورة المعلوماتية، وسوف نقسّم هذا الفصل إلى ثلاثة أقسام، نفرد القسم الأول لأركان جريمة الاحتيال بمفهومها التقليدي، أما القسم الثاني فنتناول فيه التعريف بالاحتيال الإلكتروني كأحد الجرائم المعلوماتية، ونختم الفصل بقسم ثالث نتناول فيه أركان الاحتيال الإلكتروني ووسائله، والنتائج المترتبة عليه.

1.1 أركان جريمة الاحتيال بمفهومها التقليدي:

تناول المشرّع الأردني جريمة الاحتيال في المادة (417) من قانون العقوبات الأردني رقم (16) لسنه 1960تحت عنوان : "الاحتيال وسائر ضروب الغش".

ولم تكن جريمة الاحتيال تتمتع بالاستقلالية، كجريمة منفصلة ومستقلة بطبيعتها، بل كانت مختلطة بجريمة السرقة منذ عهد القانون الروماني، والقانون الفرنسي القديم، بحيث لم تبرزْ كجريمة مستقلة إلا بعد قيامِ الثورةِ الفرنسية عام 1789، حيث باتت جريمةً مستقلةً لها أركان خاصة بها في التشريعات المعاصرة[1]، سوف نبينها في الأجزاء الآتية.

---

(1) نمور، محمد سعيد، (2007)، شرح قانون العقوبات الجرائم الواقعة على الأموال، الطبعة الأولى، دار الثقافة للنشر، عمان، الأردن، ص229. تجدر الإشارة إلى أن المشرع الأردني، عندما نظم الأحكام الخاصة بجريمة الاحتيال نص أيضاً على جرائم أخرى ملحقة بجريمة الاحتيال، وأن القاسم المشترك بين هذه الجرائم وجريمة الاحتيال أنها جميعاً تنطوي على الخداع والإيهام، وإن كانت هذه الجرائم لا تتوفر فيها جميع عناصر جريمة الاحتيال، ومن هذه الجرائم جريمة استغلال عديمي الأهلية وناقصيها، وجريمة إخفاء المعلومات،

1.1.1 التعريف بجريمة الاحتيال وعناصر ركنها المادي

إن جريمة الاحتيال، شأنها شأن باقي الجرائم، من حيث وجوب توافر أركان الجريمة الأساسية، لكي يكتمل النموذج القانوني لها.

أولاً: التعريف بجريمة الاحتيال

تنص المادة (417) من قانون العقوبات الأردني الفقرة الأولى على أن : (كل من حمّل الغير، على تسليمه مالاً منقولاً أو غير منقول، أو إسناداً تتضمن تعهداً أو إبراءً فاستولى عليها احتيالاً)

(أ) باستعمال طرق احتيالية، من شأنها إيهام المجني عليه بوجود مشروع كـــاذب، أو حادث أو أمر لا حقيقةَ لهُ، أو إحداث الأمل عند المجني عليه بحصولِ ربح وهمي، أو تسديد المبلغ الذي أُخذ بطريق الاحتيال، أو الإيهام بوجود سند دين غيرِ صحيح، أو سند مخالصة مزور أو:

(ب) بالتصرف في مال منقول أو غيرِ منقول وهو يعلم أنه ليس له صفة للتصرف به أو:

(ج) اتخاذ اسم كاذب أو صفه غيرِ صحيحة.

عوقب بالحبس من ثلاثة أشهر إلى ثلاثة سنوات وبالغرامة من مائة دينار إلى مائتي دينار.

في حين نصت الفقرة الثانية على أنه:

(أ) يعاقب بالحبس مدةً تقل عن ستة أشهر إذا ارتكب الفعل بحُجة تأمين وظيفة أو عمل في إدارة عامة.

(ب) يعاقب بالحبس مدة لا تقل عن سنتين، إذا كان مرتكب الجريمة ممن يتولون إصدار الأسهم، أو السندات، أو أي أوراق مالية أخرى،متعلقـــة بـــشركة ، أو مشروع، أو مؤسسة تجارية، أو صناعية.

ونصت الفقرة الثالثة على أنه:

وسنكتفي في هذا المقام بالحديث عن جريمة الاحتيال بمفهومها التقليدي فقط كتمهيد لمدار البحث (الاحتيال الإلكتروني) .

" تقضي المحكمة بضعف العقوبة في حال تعدد المجني عليهم".فالجاني يقوم بإيهام المجني عليه، وإيقاعه بالغلط، وحمّله على تسليم المال؛ ليستولي عليه، وبهذه الحالة فإن تسليم المال من قبل المجني عليه، ينفي عن المحتال جريمة السرقة؛ لأنه يعتبر تسليماً ناقلاً لّلحيازّة، حتى وأن كانت إرادة المجني عليه، معيبة بسبب ما وقع فيه من غلط، بفعل المحتال الذي حمّله على ذلك، ونجد غالباً أن الجاني المحتال يعتمد على المجني عليهم بتسهيل أفعالة الاحتيالية، وتعاونهم معه، معتمداً على إيهامهم، وإقناعهم بصدق أفعالهِ بشتى الوسائل التي تكون بظاهرها أعمال مشروعة، في حين أنها مبنيةٌ علّى الغش والخداع، ولذلك نلاحظ أن الجاني في الغالب ما يقوم بدراسة ضحاياه المحتملين، وانتقائهم لكي يسهلوا من مهمته الجُرمية[1].

فالاحتيال بظاهره علم وفن، ممزوجان بصورة تنال من المجتمع، دون أن تكون حِكراً على فئة معينة، أو دولةٍ دونَ سواها، فأينما وجدت المجتمعات ونشاطات الأفراد وعلاقاتهم، فمن الممكن أن نجد ضروب الاحتيال هنا وهناك، فالمحتال هو أفضلُ ممثل بارع وقادر على تقمص الشخصيات، وإتقان دوره الاحتيالي التمثيلي بصوره تجعل الاقتناع لدى الضحية، هي عنوان خسارته الفعلية للمال، وهي الغاية التي يسعى من خلالها الجاني، إلى الحصول على الربح المادي بصورة غير مشروعة، محاولاً استغلال كل ما يصب في مطامعه الاحتيالية، على حساب المجتمع والأعراف، والعقائد التي أعطت كل فرد حقه بالملكية، كما رتبها الدستور، والقوانين، وحرية انتقال هذه الملكية، ضمن الضوابط القانونية والشرعية[2].

---

(1) أبو الروس، أحمد بسيوني، (1986)، جرائم النصب، دار المطبوعات الجامعية للنشر، الإسكندرية، مصر، ص8.

(2) المدني، سليمان، (1995)، الاحتيال علم وفن، الطبعة الأولى، دار المنارة للنشر، بيروت، لبنان، ص5. تجدر الإشارة إلى أن الأثر المترتب عن الأساليب الاحتيالية، في مجال قانون العقوبات، يختلف عنه في مجال القانون المدني، بالنسبة لقانون العقوبات، فأن الأثر المترتب هو قيام المسؤولية الجنائية للجاني الذي استولى على مال الغير بطرق احتيالية، أما في القانون المدني فالأثر المترتب على ذلك الفعل هو إبطال التصرف وفسخ العقد، أنظر المواد (143،145) من القانون المدني الأردني. أحمد، عبدالرحمن توفيق، (2005)، الجرائم التي



ثانياً: عناصر الركن المادي لجريمة الاحتيال:

إن الركن المادي لجريمة الاحتيال، شأنه شأن بقية الجرائم، إذْ يشترط توافر الفعل (فعل الاحتيال) وتحقق النتيجة، وعلاقة السببية بينهما (الفعل والنتيجة)، وإن المشرّع الأّردني قد حدد أفعال الاحتيال، على سبيل الحصر، بحيث لا يُعتَبر أي استيلاءٍ على مالِ الغيرِ بغيرِ الأفعال التي حددها المشرع جريمة احتيال[1]، وهذه الأفعال نُورِدها على النحو الآتي:

أ. الطرق الاحتيالية.

وتتمثل الطرق احتيالية بقيام الجاني، بالتصرف في مال منقول، أو غيرِ منقول، وهو يعلم انه ليس له صفة التصرف به، واتخاذه اسم كاذب، أو صفة غيرِ صحيحة ونجد أن المشرع الأردني لم يضع تعريفاً للطرق الاحتيالية، شأنه شأن معظم التشريعات العربية، ولأن أيّ تعريف سوف يشوبه القصور، سيما أن مثل هذه الطرق تنطوي على الابتكار والتطور، ويشترط لقيام الفاعل لفعل من هذه الأفعال، أن تكون غايته من وراء هذا التصرف، إيهام المجني عليه وإيقاعه بالغلط، من أجل الاستيلاء على مال الغير بصورة غير مشروعه[2]، وفي قرار لمحكمة التمييز

تقع على الأموال في قانون العقوبات الأردني، الطبعة الأولى، دار وائل للنشر، عمان، الأردن، ص150.

(1) العاني، عادل إبراهيم، (1995)، جرائم الاعتداء على الأموال، الطبعة الأولى، دار الثقافة للنشر، عمان، الأردن، ص144.

(2) صالح، نائل عبدالرحمن، (1996)، الوجيز في الجرائم الواقعة على الأموال، الطبعة الأولى، دار الفكر الجامعي للنشر، عمان، الأردن، ص174. نجد أن معظم التشريعات تتفق من حيث الأفعال المكونة للركن المادي لجريمة الاحتيال، وإذا كانت اختلفت في تسمية هذه الجريمة، حيث نجد بعض التشريعات تسميها جريمة النصب، كما هو الحال في قانون العقوبات المصري رقم (58) لسنة 1937 في نص المادة (336)، أما التشريعات التي أطلقت على هذه الجريمة اسم الاحتيال، والتي أصبحت أكثر استعمالا في كثير من التشريعات ومنها قانون العقوبات الأردني لسنة 1960 في نص المادة (417)، وقانون العقوبات العراقي، رقم (111) لسنة 1969 في نص المادة (456)، وغيرها من التشريعات، فالتوافق موجود وأن اختلفت التسميات الجيوشي، طاهر خليل، (2001)، جرائم

الأردنية حيث قضت أنه : "ثبت بالبيانات الواردة في الدعوى أن المحكوم عليه قد ادعى لدى المشتكين بأنه يحمل وكالة بيع قطعة ارض، وأجرى الكشف عليها معهم، وأطلعهم على مخططها في البلدية، فانخدع المشتكون بأقواله، وسلموه عشرينَ ألفَ دينار من ثمنها، على أن يُتمَ مُعَاملة الفراغ في اليوم التالي، وبما أن المحكوم عليه انتحل صفة وكيل مالك الأرض، وأنه صاحب مكتب عقاري، فيتحقق البند الثالث من نص المادة (417) من قانون العقوبات فضلاً، عن قيامه بالكشف على موقع الأرض، واطلاع المشتكين على مخططها لدى البلدية، فهذه الأفعال معززة لكذبه، بما يعني أنها تشكل ركناً من أركان جريمة الاحتيال ولم يكن فعله مجرد كذب"[1].

فبات البابُ مفتوحاً أمام فقهاء وشُرّاح القانون، أن يسهموا بحسب اجتهاداتهم وتفسيرهم، بسبب سكوت المشرّع في نصوصه، عن وضع تعريف محدد لهذه الطرق الاحتيالية، من أجل رسم مفهومٍ واضحٍ وشمولي قدر المستطاع لهذه الطرق؛ لما لها من أهمية بالغة في تحديدِ إذا ما كانت هذه الأفعال الصادرة من الأشخاص، هي أفعال مجرمة أو غير ذلك، والتي من خلالها، يتبين إذا ما كان من المفروض تطبيق نصوص القانون على هذه الأفعال من عدمه[2].

فقد عرف جانب من الفقه الفرنسي، والبلجيكي الطرق الاحتيالية بأنها : كذبٌ مدعمٌ بأفعال مادية أو بوقائعَ خارجية، أو أخراج أو تمثيل مسرحي، يجعل الكذب وكأنه حقيقة، و إذا نظرنا إلى الفقه المصري، نجد جانب من الفقه لم يبتعد كثيراً عن باقي التعريفات للطرق الاحتيالية، وعَرّفَ هّذه الطرق الاحتيالية على : أنها إدعاءاتُ

الاحتيال الأساليب والوقاية والمكافحة، الطبعة الأولى، أكاديمية نايف للعلوم الأمنية، الرياض، السعودية، ص28.

(1) قرار محكمة التمييز الأردنية بصفتها الجزائية رقم 1987/110 (هيئة خماسية) تاريخ 1987/4/28، منشورات مركز عدالة.

(2) البطراوي، عبدالوهاب، (2007)، شرح جرائم ضد الأموال، الطبعة الأولى، جامعة العلوم التطبيقية، البحرين، ص170.

كاذبةٌ تدعمها مظاهر كذابة أو أعمال خارجية، من شأنها حمّل المجني عليه على التصديق وتسليم المال(1)، وعليه فإن الطرق الاحتيالية تستلزم من الشروط ما يلي:

(أ) الكذب:

الاحتيال يستند على الغش والخداع، وقوامهما الكذب، وهو الذي يعمل على تغيير الحقيقة بواقعة كاذبة، يجعل منها مطابقة للحقيقة بهدف إيقاع المجني عليه بالغلط، فيقتنع المجني عليه بحقيقة هذه الصورة الكاذبة، وهو بالحقيقة يضر به هذا التصرف الذي يعتقد بصحته، علماً بأنه مبني على الكذب من قبل المحتال (الجاني)(2)، إذْ أن الكذب هو تغيير للحقيقة، أي جعل واقعة كاذبة في صورة واقعة صحيحة، سواء أكان ذلك الكذب بالكتابة، أو شفوياً، أو بالإيحاء، أو بالإشارة لدلالات معينة، ومعرفته سو اء كان الكذب كلياً أو جزئياً، ولكن الكذب بحد ذاته، لا يكفي لقيام جريمة الاحتيال، إذْ يتوجبُ أن يتم تدعيم الكذب أيضاً بما يسمى بالمظاهر الخارجية(3).

(ب) المظاهر الخارجية:

أن وجود المظاهر الخارجية، تعمل على تعزيز كذب الجاني المحتال، والتي تدفع الآخرين إلى ضرورة الاعتقاد بصحة أقوال الجاني المحتال، وهذه المظاهر الخارجية، التي يلجأ إليها الجاني كثيرة ومتنوعة، ومن الصعب حصرها، في حين حددتْ بعضُ التشريعات بعض هذه الصور للمظاهر الخارجية المدعمه للكذب، ونذكر من هذه المظاهر:

(1) القيام ببعض الأعمال المادية.

(2) الاستعانة بالغير.

---

(1) بهنام، رمسيس، (1982)، القسم الخاص في قانون العقوبات، دار المعارف للنشر، الإسكندرية، مصر، ص507.

(2) صالح، نائل عبدالرحمن، (1996)، شرح قانون العقوبات القسم الخاص الجرائم الواقعة على الأموال، دار الفكر الجامعي للنشر، عمان، الأردن، ص173.

(3) حافظ، مجدي محب، (2000)، جرائم النصب والاحتيال والجرائم الملحقة بها، دار الكتب القانونية للنشر، الإسكندرية، مصر، ص35.

(3) كالجاني حائزاً لصفّه تحمل الآخرين على الثقة فيه[1]. وأن التشريعات اختلفت فيما بينها، في تحديد الغاية والأغراض التي تستهدفها مثل هذه الطرق الاحتيالية، ونذكر من هذه التشريعات التي لم تعهد لنفسها تحديد هذه الإغراض، والغاية من الطرق الاحتيالية بنصوص قانونية، قانون العقوبات العراقي في نص المادة (456)، والقانون الايطالي في نص المادة (460)، والقانون السويسري في نص المادة (148)، والقانون السوداني في نص المادة (357) وغيرها من التشريعات[2].

في حين أن بعض التشريعات حددت هذه الإغراض والغاية، ونذكر منها قانون العقوبات الأردني في نص المادة (417)، وقانون العقوبات الفرنسي بنص المادة (405)، والقانون المغربي في نص المادة (336) وغيرها من تشريعات الدول[3].

أن المادة (417) من قانون العقوبات الأردني، تطلبت أن يكون من شأن هذه الطرق الاحتيالية، إيهام المجني عليه وإيقاعه بالغلط بحيث بات من الممكن أن نُعرّف الإيهام على أنّه : إيقاع الشخص في غلط، وحمله على تكوين اعتقاد مخالف للواقع بوجود هذا الأمر، وقد حددت نص المادة (417) صور الإيهام على النحو التالي:

(أ) الإيهام بوجود مشروع كاذب: بحيث يقوم الجاني بإيهام المجني عليه، بوجود مشروع كاذب وهمي غير موجود، كوجود شركة أو جمعية تمارس نشاطاً معيناً، كأن يقوم هذا الجاني باستئجار شقه، ويقوم بتأثيثها كمقر لهذا المشروع

---

(1) البحر، ممدوح خليل، (2008)، الجرائم الواقعة على الأموال في قانون العقوبات الإماراتي، الطبعة الأولى، دار أثراء للنشر، عمان، الأردن، ص200.

(2) جعفر، علي محمد، (2006)، قانون العقوبات القسم الخاص، الطبعة الأولى، دار مجد للنشر، بيروت، لبنان، 179.

(3) نمور، شرح قانون العقوبات، الجرائم الواقعة على الأموال، ص245.

الوهمي، من أجل أن يتولد لدى المجني عليه، قناعة بصدق أقوال وأفعال هذا الجاني[1].

(ب)الإيهام بوجودِ حادثٍ أو أمر لا حقيقة له: ويُقصد بذلك حمل المجني عليه بالاعتقاد بوجود أمر لا وجود له أصلاً، أو غير موجود بالصورة التي يتخيلها المجني عليه، وهذا يشمل كل إيهام بأمر يختلف عن حقيقته، ونستشهد بذلك بما ورد بقرار محكمة التمييز الأردنية "إذا لم يكن إقدام المتهم، على استعمال السند بقصد الاحتجاج به ضد الشخص الذي جرى تزوير إمضائه، وإنما كان بقصد اتخاذ السند وسيلة لإيهام الغير، بوجود أمر لا حقيقة له وحمله على تسليمه مالاً، فإنه سواء أكان الاستعمال لدى جهة رسمية، أو خاصة لا يشكل جريمة استعمال سند مزور بالمعنى المنصوص عليه في المادة 261 من قانون العقوبات، وإنما هو عنصر من عناصر جريمة الاحتيال، خلافاً لنص المادة 417 "[2].

(ج)إحداث الأمل بحصولِ رِبحٍ وهمي : بحيث يقوم الجاني بإيهام المجني عليه بمقدرته على تحقيق ربح له في المستقبل، من خلال صفقه معينه، أو شيء يرغب المجني عليه بالحصول عليه، سواء أكان هذا الربح مادي أو ربح معنوي، مثل أن يزوجه امرأة ذات سلطه أو يوليه منصب معين.

---

(1) مراد، عبد الفتاح، (1996)، شرح جرائم النصب وخيانة الأمانة والجرائم الملحقة بها، الطبعة الأولى، دار الفتح للنشر، القاهرة، مصر، ص49، قضت محكمة التمييز الأردنية أنه: "يشترط في جريمة الاحتيال أن يأتي الجاني فعلاً ايجابياً ينتحل به الاسم الكاذب، أما إذا اتخذ موقفاً سلبياً بأن ترك الغير يعتقد في صفه ليست له، أو اسماً غير اسمه، واستطاع الحصول بذلك على المال، فلا يتوافر بذلك ركن الجريمة ويكون من سلم المال قد فرط في حق نفسه". قرار رقم 1976/42 منشورات مركز عداله.

(2) قرار محكمة التمييز الأردنية بصفتها الجزائية رقم 1970/52 (هيئة خماسية) تاريخ 1970/1/1، منشورات مركز عدالة.

(د) إحداث الأمل بتسديد المبلغ الذي أخُذ بطُريق الاحتيال : بمعنى أن الجاني قد تسلم المال من المجني عليه، ولكن يسعى إلى إيهامه أنّه سوف يعيد له المال، فيقوم بإيهامه بغية الاحتفاظ بالمال بالاحتيال عليه مرة أخرى[1].

(هـ) الإيهام بوجود سند دين غير صحيح : بحيث يحاول الجاني إيهام المجني عليه وإقناعه، أنه يمتلك سند دين يطالبه به علماً أن السند مزور بحقيقته.

(و) الإيهام بوجود سند مخالصة مزور : وتتمثل بإظهار الجاني سند مخالصة مزور، أي غير سليم أو الادعاء بامتلاكه، مع أنّه لا وجود لمثل هذا السند[2].

ثانياً: التصرف دون حق في مال مملوك للغير: وقد تم الإشارة إلى هذه الصورة في صور الركن المادي لجريمة الاحتيال المشار إليها في نص المادة (417) من قانون العقوبات الأردني في الفقرة أ/ب حيث جاء بها:

"بالتصرف في مال منقول، أو غير منقول، وهو يعلم أنه ليس له صفة للتصرف به"، بحيث أن المشرّع الأردني قد خالف بعض التشريعات، التي قصرت التجريم بالأموال المنقولة فقط، مثل التشريع المصري، ليوسع بذلك الدائرة الاحتيالية لتشمل الأموال المنقولة، وغير المنقولة ففي هذه الصورة، إن المجني عليه هو في الأساس ليس مالك للمال المنقول، أو غير المنقول الذي تعلق تصرف الجاني به، أنما وقع ضحية خداع الجاني، الذي أوهمه أن لديه المقدرة على أن ينقل إليه حقوقاً على هذا المال، ونتيجة لهذا الاعتقاد الخاطئ من قبل المجني عليه، قام بتسليم المال إلى الجاني، وبناء عليه يتوجب توافر عنصرين لقيام هذه الصورة[3]:.

(أ) أن يكون التصرف في مال منقول أو غير منقول، ويكون ذلك بصورة نقل ملكية عقار، أو منقول، أو ترتيب حقٍ عيني على هذا المال، بحيث لا يشمل عقود البيع فقط، بل كافة التصرفات للحقوق العينية الأصلية والتبعية، ويُستثنى

(1) عبد الغني، سمير، (2007)، جرائم الاعتداء على الأموال، دار شتات للنشر، القاهرة، مصر، ص225.

(2) نمور، شرح قانون العقوبات، الجرائم الواقعة على الأموال، ص255، 256.

(3) هرجة، مصطفى مجدي، (2004)، جرائم النصب وخيانة الأمانة والجرائم المرتبطة، دار محمود للنشر، الإسكندرية، مصر، ص39 وما بعدها.

من ذلك الأعمال الإدارية مثل :الإيجار سواء أكان شكل التصرف مكتوبــاً، أو شفوياً، ويتم إثباته وفقاً لقواعد الإثبات المنصوص عليها في قــانون أصــول المحاكمات الجزائية، لأنها واقعة جزائية وليست مدنية، ويتم إثبات التــصرف في هذه الحالة بكافةوسائل الإثبات، حسب ما نصت عليه المواد (72،73) من القانون المدني الأردني[1].

(ب) أن لا يكون للجاني صفة للتصرف بالمال بحيث لا يكون للجــاني أي حــق بالقيام بمثل هذا التصرف؛ لأنه ليس مالك لهذا المال وقد يكون المال في حوزة هذا الجاني دون وجه حق ويقوم بالتصرف فيه لصالح المجني عليــه بقــصد الاحتيال عليه وتسلمه المال ، وهو عالمٌ بأن هذا يعتبر اعتداء على حق ملكية الغير[2].

ب. اتخاذ اسم كاذب أو صفة غير صحيحة

إن الجاني قد يلجأ إلى اتخاذ اسم كاذب، من أجل تدعيم طرقه الاحتيالية، وأنّ اتخاذ الجاني الاسم الكاذب وحده يكفي لقيام الركن المادي لجريمة الاحتيــال، فقــد ينسب لنفسه اسماً مستعاراً غير اسمه الحقيقي، سواء أكان اسم لشخص آخر أو اسم وهمي اختلقه لنفسه والأمر سيان، إذا أتخذ الاسم كله بشكل كامل، أو جزءً منه، كأن يغير اسمه ويبقي على اسم العائلة الحقيقي، أو أن يغير اسمه واسم العائلة وهكــذا، ولكن لا يُعَد الشخص متخذاً لاسم كاذب، إذا كان يطلق عليه اسم مشهور به عرفــاً في الوسط المجتمعي، وكناية متعارف عليه سوا أكان هو من اطلق على نفسه هــذا اللقب، أو من قبل أقاربه، أو أبناء المنطقة التي يقطنها[3].

أما الصفة غير الصحيحة، فإنّ المشرّع لم يحدد المقصود بها، ولكن يمكــن القول أن الصفة تجمع المركز الذي يشغله الشخص، أو الوظيفــة، أو الحرفــة، أو

---

(1) الجيوشي، جرائم الاحتيال الأساليب والوقاية والمكافحة، ص56 وما بعدها.

(2) الشاذلي، فتوح عبد الله، (1996)، جرائم الاعتداء على الأشخاص والأموال، دار المطبوعات الجامعية للنشر، الإسكندرية، مصر، ص548.

(3) الجبور، محمد، (1997)، الجرائم الواقعة على الأموال، الطبعة الأولى، دار الثقافة للنشر، عمان، الأردن، ص191.



مكانته وهكذا، بحيث من الممكن أن يدعي الجاني أنّه يشتغل بمنصب وظيفي معين[1].

فقد جاء في أحد قرارات محكمة التمييز الأردنية أنّه : " إذا أرسل المشتكى عليه سيارتين لا ستلام الطحين، من الموظف المختص بتسلمه، وإيهامه أن السائقين موفدان من المتعهد لاستلام الطحين ونقله بالسيارتين، وسلم الطحين تحت تأثير هذا الإيهام، وتمكن المشتكى عليه من الاستيلاء عليه بهذه الوسيلة، فإن فعله يشكل احتيالاً وينطبق عليه نص المادة (417)"[2]، وقد يدعي الجاني بوجود علاقة قرابة، أو مصاهرة بينه وبين إحدى الشخصيات البارزة، وقد يأتي الادعاء بصفة غير صحية أيضاً، كمن يدعي أنه موظف كبير لدى إحدى المؤسسات أو البنوك، وهو في الحقيقة موظف صغير ولكنه ينتحل هذه الصفة؛ ليضيف لنفسه المزيد من نفوذ وصلاحيات هذه الشخصية، من أجل تحقيق مبتغاه وارتكاب جريمة الاحتيال، وهذه الصفات التي قد يتخذها الجاني في انتحال الصفة غير الصحيحة، لا حصر لها، خصوصاً أن مثل هذا النوع من الجرائم الاحتيالية، دائماً ما يقوم على الابتكار والتطور، لكي يستطيع مجاراة تطور الحياة المجتمعية[3].

ومع ذلك، نجد أنه يجب أن تتوفر عده شروط للاحتيال، باستخدام اسم كاذب أو صفة غير صحيحة نُورِدُها على النحو الآتي:

(1) أن يكون الإدعاء بالاسم أو الصفة، من شأنها أن تؤدي إلى خِداع المجني عليه وإيقاعه بالغلط.

(2) أن يصدر هذا العمل، من خلال سلوك ايجابي، يمارَس وَيَصدُر من قبل الجاني نفسه.

---

(1) توفيق، عبدالرحمن؛ ونجم، محمد صبحي، (1983)، شرح قانون العقوبات الأردني، الجزء الأول، الطبعة الأولى، دار التوفيق للنشر، عمان، الأردن، ص131.

(2) قرار محكمة التمييز الأردنية بصفتها الجزائية رقم 1968/31 (هيئة خماسية)، منشورات مركز عدالة.

(3) الجبور، الجرائم الواقعة على الأموال، ص191.



(3) ألاّ يكونّ الادعاء ظاهر الكذب، بحيث يكتشفه الشخص العـادي، بـل يكون منطوي على حيلة ليس من السهل اكتشافها[1].

ثالثاً: النتيجة الإجرامية (تسليم المال)

إن المادة (417) من قانون العقوبات الأردني، جرّمت فعل كل مـن يقـوم بالاستيلاء على مال منقول، أو غير منقول بطرق احتيالية، والاستيلاء يـتم بتـسليم المال للجاني، الذي يُعتبر نتيجة جرميه للنشاط الايجابي، الذي صدر من قبل الجاني تجاه المجني عليه، فما المقصود إذاً بالتسليم والشروط الواجب توافرها لقيام جريمة الاحتيال، بما أن تسليم المال إلى الجاني، يعتبـر مـن أهـم العناصـر المكونـة للجريمة[2]، فالتسليم: هو قيام المجني عليه، أو من يعمل لحسابه، بتسليم المال نتيجة للغلط الذي وقع به المجني عليه، بسبب الطرق الاحتيالية التي اسـتخدمها الجـاني لإيهامه بتسليم المال، فالتسليم قد يكون بشكل مباشر، من قبل المجني عليه، أو مـن قبل شخص آخر يعمل لحسابه، وهذا الشخص ما هو إلا منفذ لأوامر المجني عليه، ولا يُسأل جنائياً، مادام أنه حسن النية وليس له صله أو أي اتفاق مع الجاني[3].

شروط التسليم:

(1) يجب أن يكون الأسلوب والطرق الاحتيالية، التي استخدمها الجـاني، هـي الأساس الذي ارتكز عليه تسليم المال من المجني عليه للجاني، ولولا وجود هذه الطرق الاحتيالية، لما قام المجني علية بتسليم المال إلى الجاني.

(2) اتجاه إرادة المجني عليه، المبنية على الطرق الاحتيالية المستخدمة من قبـل الجاني، هي الدافع إلى تسليم المال، دون النظر إلى الأسلوب الذي تـم بـه التسليم سواء أكان مباشراً أو غيرَ مباشر.

(3) أن يكون الشخص الذي سلم المال، أو أمر بتسليمه، هو ذات الشخص الـذي وقع نتيجة لهذه الجريمة الاحتيالية، وأن يكون هدف الجاني لحظـة تـسلمه

---

(1) أبو خطوة، أحمد، (1990)، الجرائم الواقعة على الأموال، الطبعة الأولى، دار البيان للنشر، دبي، الإمارات، ص195.

(2) مراد، شرح جرائم النصب وخيانة الأمانة والجرائم الملحقة بها، ص58.

(3) الجبور، الجرائم الواقعة على الأموال، ص195.

المال من المجني عليه، هو نية تملك هذا المال، والاستيلاء عليه بغض النظر عن الباعث، أما إذ لم تتولد لديه نية التملك فإنّها تُخرجِه من دائرة التجريم[1].

(4) يجب أن يكون التسليم لاحقاً، على استخدام الطرق الاحتيالية لا سابقاً عليها، بحيث يقوم المجني عليه، بتسليم الجاني المال، بعد استخدام هذا الأخير، طرق احتيالية بحق المجني عليه[2].

والجدير بالذكر أنّه لا تأثير على التسليم، إذا كان المجني عليه غير مالك للمال، بل يكفي أن يكون حائزاً لهذا المال وبعهدته، وهو المسؤول والمحاسب على هلاك أو فقدان هذا المال، وبخصوص طبيعة المال محل جريمة الاحتيال، بالرجوع إلى نص المادة (417) من قانون العقوبات الأردني نجد أن المشرّع قد حدد موضوع الاحتيال، وما يصلح أن يعد مال، عندما نص على أنّه : (كل من حمّل الغير على تسليمه مالاً منقولاً، أو غير منقول، أو أسناداً تتضمن تعهداً، أو إبراءً فاستولى عليها احتيالاً ...)، أي أن جريمة الاحتيال، قد تقع على منقول، أو عقار على خلاف نص المادة (336) من قانون العقوبات المصري، والتي دلت بشكل واضح وصريح على أن جريمة الاحتيال، لا تقع إلا على منقول، وعدم إمكانية وقوعها على كل ما هو غير منقول بنص لا يقبل الاجتهاد[3].

فمن استولى على شيء ليس له صفة المال، لا يمكن اعتبار فعله احتيالاً، وإن كان قد توصل إليه عن طريق الحيلة والخداع، فمن خادع فتاة واصطحبها مستخدماً طرق احتيالية وقام بمواقعتها، فأنه لا يعتبر مرتكب لجريمة الاحتيال، كما بينت نص المادة (417) أن المال يجب أن يكون مملوك للغير، وليس للجاني، وهذا هو الحال نفسه الذي يُشترُط في المال محل جريمة السرقة ، من حيث ملكية المال،

---

(1) حافظ، جرائم النصب والاحتيال والجرائم الملحقة بها، ص180 وما بعدها.

(2) البطراوي، شرح جرائم ضد الأموال، ص186.

(3) جعفر، قانون العقوبات القسم الخاص، ص105 وما بعددها.

وتصنيفها ضمن الجرائم الواقعة على الأموال [(1)]، كما أن المال، يجب أن يكون ذا قيمة مادية في كلا الجريمتين، ويكفي لقيام جريمة الاحتيال، أن يكون المال له قيمة أدبية، أو معنوية للمجني عليه، لان الشيء الذي له قيمة معنوية، يصح أن يكون محلاً للملكية والاستيلاء عليه، باستخدام الطرق الاحتيالية، وإن كان جانب من الفقه اتجه إلى أن المال، يجب أن يكون ذا قيمة مادية فقط، ولا مكان للقيمة المعنوية له، ما دام أنه لا يتمتع بالقيمة المادية ليعتبر مال، والاستيلاء علية بالطرق الاحتيالية لا يجعل منه محلاً للجريمة[(2)].

ولكن الرأي الراجح والمعمول به في الغالب، أن المال سوا أكان ذا قيمة معنوية أو قيمة أدبية، يصلح بأن يكون محلاً لجريمة الاحتيال، ما دامت قد ثبتت له صفة المال، ويأتي هذا من باب حرص المشرع، بتوفير حماية أكبر لحقوق الأفراد وممتلكاتهم، وسد أي ثغرات من شأنها، أن تكون ذريعة يحتج بها مرتكبو جرائم الاحتيال، عند قيامهم بارتكاب أفعالهم المجرمة[(3)].

وفي حال تحقق كل من الركن المادي لجريمة الاحتيال، والركن المعنوي، فإن الجريمة لا تخرج بإطارها الكامل، بل لا بد لها من صله ورابطة بين هذين

---

(1) أبو خطوة، الجرائم الواقعة على الأموال، ص207. جاء في قرار لمحكمة التمييز الأردنية: "أنه لا يشكل طلاء الأساور الفضية بالذهب، بقصد التزييف جناية تزييف المسكوكات خلافاً للمادة (274) من قانون العقوبات، لان عبارة المسكوكات لا تنطبق إلا على العملات المعدنية، ولا تشمل المصاغ، ويكون الجرم بفرض ثبوته جنحة الاحتيال، وبالتالي يكون الاختصاص منعقداً لمدعي عام محكمة البداية، وليس لمدعي عام محكمة أمن الدولة". قرار رقم 1994/475 منشورات مركز عداله. وتجدر الإشارة إلى أن القضاء الفرنسي، لم يشترط حدوث الضرر في جريمة الاحتيال، وأن الركن المادي للجريمة يكتمل بمجرد وقوع فعل الاحتيال، والاستيلاء، وقد قضى ّبأن جريمة النصب تقع إذا حمل البائع المشتري بطرق احتيالية على الشراء، ولو كان الذي اشتراه مساوي لقيمة ما دفعه تقريباً. محمد، عوض، (1987)، جرائم الأشخاص والأموال، دار المطبوعات الجامعية، الإسكندرية، مصر، ص396.

(2) أبو خطوة، الجرائم الواقعة على الأموال، ص209.

(3) نمور، شرح قانون العقوبات، الجرائم الواقعة على الأموال، ص280.

الركنيين، لتكوين الجريمة، وهذا ما يسمى بعلاقة السببية، بحيث يتوجب أن تكون هنالك علاقة سببية بين الطرق والأساليب الاحتيالية، التي استخدمها الجاني، وبين النتيجة الجرمية المتحققةِ، بتسليم المجني عليه المال للجاني، بحيث يكون هذا التسليم، هو نتاج هذه الطرق والأساليب الاحتيالية، التي استخدمها الجاني للاستيلاء على المال، ومن أجل قيام علاقة السببية بين الفعل والنتيجة، واعتبار تسليم المال جاء كنتيجة حتمية لفعل الجاني[1]، وعليه ينبغي توافر الشروط الآتية:

(1) أن يقوم الجاني بأحد الأفعال الاحتيالية، التي نصت عليها المادة (417) من قانون العقوبات الأ ردني، والمدعمة بالمظاهر الخارجية اللازمة لقيام الركن المادي للجريمة، من خلال استخدامه الطرق الاحتيالية.

(2) يتوجب أن يكون تسليم المال لاحقاً، على استعمال الطرق والأساليب الاحتيالية (نشاط الجاني).

(3) أن يترتب على استعمال الجاني لهذه الطرق الاحتيالية، وقوع المجني عليه بالغلط، وإيهامه من خلال إقناع المجني عليه، بإدعاءات الجاني، ويقوم بهذه الحالة بتسليم الجاني المال، مقتنع بصحة أكاذيب الجاني، التي توصله إلى كسب مال الغير[2].

فالإيهامُ بأمرٍ: هو إيقاع الشخص في الغلط، أو حمله على تكوين اعتقاد مخالف لواقع هذا الأمر، ومن أجل الوصول إلى النتيجة الإجرامية، لابد أن تكون هذه الأفعال على درجة من الإتقان، بغية خداع المجني عليهم[3]، ولكن ما هو المعيار المعتمد لهذا الإيهام؟

ذهب رأي إلى الأخذ بالمعيار الموضوعي، حيث أنّه لا يكفي لتحقيق معنى الإيهام، أن ينخدع المجني عليه بإدعاءات الجاني وأكاذيبه، بل يلزم أن تكون هذه الأكاذيب المرافقة للمظاهر الخارجية، على درجة من الإتقان، بحيث ينخدع بها

(1) المنشاوي، عبدالحميد، (1990)، جرائم النصب والاحتيال في ضوء القضاء والفقه، دار الفكر الجامعي، الإسكندرية، مصر، ص64.

(2) توفيق ونجم، شرح قانون العقوبات الأردني، ص122.

(3) نمور، شرح قانون العقوبات، الجرائم الواقعة على الأموال، ص248.

الأشخاص العاديون متوسطو الذكاء، وعليه إذا كانت الطرق الاحتيالية التي استخدمها الجاني، من شأنها أن يكتشف أمرها الشخص العادي متوسط الذكاء، فأن ذلك لا يكفي لتحقيق معنى الإيهام، ولا يصلح لقيام جريمة الاحتيال؛ لأن الإنسان يجب أن يكون حذر في تعاملاته مع الآخرين، وقد أخذ بهذا الرأي القضاء الفرنسي في بداية الأمر[1].

ولكن الرأي الراجح هو الأخذ بالمعيار الشخصي، وهو ينظر إلى الإيهام من خلال وجهة نظر شخصية لا موضوعيه، بمعنى أنه يكفي لتحقيق الإيهام، أن ينخدع المجني عليه فعلاً بالأكاذيب الصادرة عن الجاني، والمدعمة بالمظاهر الخارجية، وينظر إلى الإيهام بقدر تأثير هذه الأفعال بالمجني عليه، وهذا المعيار ينسجم مع الطبيعة القانونية للجزاء، بتوفير حماية أكبر للحقوق، وهو المعيار الذي أخذ به المشرع الأردني من خلال نص المادة (417).

وفي قرار لمحكمة التمييز الأردنية " إن المتهم، إذا لم يظهر بأي مظهر خاص به يميزه عن عامة الناس، ومن شأنه التأثير في نفس المشتكي، فإنّ فعله لا يرقى إلى درجة التدليس الجنائي، لأنه لم يدعم قوله بأي مظهر خارجي، ولا بأية وثيقة من شأنها أن تخدع أحد بمزاعمه"[2].

رابعاً: الشروع في جريمة الاحتيال التقليدية

للحديث عن الشروع، لابد لنا أولا من معرفة المقصود بالشروع، وكيف تناوله المشرّع الأردني، حيث نظم أحكامه في المواد (68_71) من قانون العقوبات وفرق المشرّع بين نوعين من الشروع، فجاء بنص المادة (68) تعريف الشروع الناقص، عندما عرّفهّ على أنّه : "هو البدء في تنفيذ فعل من الأفعال الظاهرة، المؤدية إلى ارتكاب جناية أو جنحة، فإذا لم يتمكن الفاعل من إتمام الأفعال اللازمة، لحصول تلك الجناية أو الجنحة، لحيلولة أسباب لا دخل لإرادته فيها، عُوقِب على النحو الآتي إلا إذْ نص القانون على خلاف ذلك".

---

(1) حافظ، جرائم النصب والاحتيال والجرائم الملحقة بها ص194.

(2) قرار محكمة التمييز الأردنية بصفتها الجزائية رقم 1976/13، (هيئة خماسية)، بتاريخ 1976/1/1، منشورات مركز عداله.

في حين تناولت المادة (70) تعريف الشروع التام حيث عرّفتهّ على أنّــهّ : " إذا كانت الأفعال اللازمة لإتمام الجريمة، قد تمت ولكن لحيلولة أسـباب مانعــة لا دخل لإرادة فاعلها فيها، لم تتم الجريمة المقصودة عُوقِب على الوجه الآتي..."

وتجدر الإشارة أن المشرّع الأردني لم يكن يُعاقِب على الـشروع بجريمـة الاحتيال، حتى صدور القانون، رقم (9) لسنة 1988 المعدل لقانون العقوبات، حيث أورد بالفقرة الثالثة في نص المادة (417) بموجب المادة (15) من قانون التعـديل أنّه: " يُطبق العقاب نفسه على الشروع في ارتكاب أي من الجنح المنصوص عليها في هذه المادة"

وعليه فإنه متى قام المجني عليه، بتسليم المال إلى الجاني، بناءً على إحدى الوسائل الاحتيالية المبنية، على الغش والخداع فإن جريمة الاحتيال تقـع، وبالتـالي توقع العقوبة المحددة على الجاني[1]، أما إذا لم يحصل تسليم للمال، بالرغم من بدء الجاني باستخدام إحدى الوسائل الاحتيالية، وكان عدم التسليم، راجع لـسبب خـارج عن إرادة الجاني، إذْ يُعتبر بهذه الحالة شروع تام في ارتكاب الجريمـة، فمعيـار الشروع في الاحتيال هو السعي إلى الاتصال بالمجني عليــه وخداعــه وبتجـريم المشرّع للشروع في جريمة الاحتيال، فأنّه سَد الفراغ التشريعي السابق في قـانون العقوبات، وسار على نهج غالبية التشريعات، إذْ أنّه من غير المتصور عدم التجريم على الشروع، لأنه سوف يؤدي إلى إفلات الكثير مــن المجـرمين مــن الجــزاء، بالإضافة إلى أن الـ مشرع الأردني، قد ساوى في النــصوص الخاصــة، بجريمــة الاحتيال في العقاب بين الجريمة التامة للاحتيال، والشروع فيها في محاولــة منــه للتعريف بحجم الجرم الذي يقدم عليه الفاعل، والحد من ارتكاب هذه الجرائم[2].

وغالباً ما يتمثل الشروع في جريمة الاحتيال، عندما يتنبــه المجنــي عليــه ويفطن للأساليب الاحتيالية، التي يعهد الجاني ممارستها عليه فيمتنع عن تسليم المال لهذا الجاني، وقد يتحقق الشروع أيضاً، في الحالة التي يكتشف فيها المجنــي عليــه خداع الجاني ومع ذلك، يقوم بتسليم المال إلى الجاني تحت تأثير عامل آخــر غيــر

---

(1) نمور، شرح قانون العقوبات الجرائم الواقعة على الأموال، ص276.

(2) العاني، جرائم الاعتداء على الأموال، ص188.

الوسائل الاحتيالية،التي مارسها الجاني [1]، ومن الأمثلة على ذلك، قيام أحد الجُناة بإيهام شخص أنّه صاحب شركة مالية لتداول الأسهم بالبورصات العالمية، وحثه على تسليم المال إليه على أساس أنها ثمن شراء لهذه الأسهم، التي سوف تدر له الربح الوفير، فيتنبه المجني عليه لهذه الحيلة، ولكن الجاني يدعم أكاذيبه بالاستعانة ببعض الأشخاص، فيقوم المجني عليه بتسليم المال إلى الجاني خوفاً من هؤلاء الأشخاص، فالجاني في هذه الحالة يُعَدُ شارعاً في جريمة الاحتيال، بالرغم من تسلمه المال؛ وذلك لأن التسليم لم يكون نتيجة الأفعال الاحتيالية التي مارسها الجاني، بل راجعاً إلى سبب آخر لا دخل له بهذه الوسيلة[2]..

ونجد أنّه من غيرِ المتصورِ الشروع في جريمة الاحتيال، إذا كانت الأفعال الاحتيالية التي يمارسها الجاني غير معقولة أو منطقيه، بحيثُ أنها من المستحيل أن توقع أي شخص عادي بالغلط وإيهامه لينخدع بها، كما لو كانت هذه الوسائلُ ساذجةً ومكشوفةً بطريقة فاضحة للجميع، مثل أن يدعي شخص النبوة ويطالب بمزايا هذه الصفة ليمارس أفعاله الاحتيالية من خلالها، أو كمن يدعي أنه أحد الإبطال المشهورين المتوفين، ويطالب بمزايا هذه الصفة لتنفيذ جرمه الاحتيالي، فإنّه في هذه الحالة تنتفي العلة التي على أساسها حدد العقاب على الشروع[3].

ومن التشريعات أيضاً التي ساوت في العقوبة، بين الجريمة التامة للاحتيال وبين الشروع فيها، دولة الإمارات العربية المتحدة، حيث نظم قانون العقوبات الاتحادي رقم 13 لسنة 1987، جريمة الاحتيال في نص المادة (399) حيث تناولت الفقرة الثالثة (ج) على أنّه: "يعاقب على الشروع في الاحتيال بالحبس مدة لا تزيد على سنتين، أو بالغرامة التي لا تزيد على عشرين ألف درهم".

وبحسب رأي الباحث، أن التشريعات التي ساوت بالعقاب، بين الجريمة التامة والشروع بها وعلى رأسها التشريع الأردني، قد ساهمت بشكل فعلي، بالحد من ارتكاب جرائم الاحتيال والشروع بها، حيث أنها لم تضع عقوبة مخففة للشروع،

---

(1) عبدالغني، جرائم الاعتداء على الأموال، ص289.

(2) صالح، الوجيز في الجرائم الواقعة على الأموال، ص182.

(3) البطراوي، شرح جرائم ضد الأموال، ص198 وما بعدها.

في دلالة منها على خطورة هذه الأفعال، (الشروع) التي إذْ استمرت تُخْرِج جريمة الاحتيال إلى حيز الوجود، لما لهذه الجرائم من أضرار جسيمة على حقوق الأفراد والمجتمع، كونها تندرج ضمن الجرائم الواقعة على الأموال.

2.1.1 الركن المعنوي لجريمة الاحتيال

جريمة الاحتيال من الجرائم القصدية، التي لابد لقيامها من توافر القصد الجرمي العام، المتضمن عنصرين أساسيين هما : العلم والإرادة، ووجوب توافر القصد الخاص، المتمثل في نية التملك للمال محل الجريمة، بحيث أنّه لا وجود لجريمة الاحتيال، من غير توافر القصد الجرمي للفاعل، بحيث تتجه أرادة الجاني، إلى الاستيلاء على مال الغير، بهدف تملكه، مستخدماً الأساليب الاحتيالية، والخداع في جريمة الاحتيال، شأنها شأن جريمة السرقة بحيثُ لا يكفي القصد الجرمي العام لقيامها، بل يتوجب أيضاً توافر القصد الجرمي الخاص (نية التملك) لقيامها[1].

أولاً: القصد العام:

ومثل هذا القصد، يجب توافره في جميع الجرائم القصدية، والمتمثل في اتجاه إرادة الجاني للقيام بالتصرف، والنشاط الجرمي، وتحقيق النتيجة الجرمية، بالرغم من معرفته بكافة عناصر الجريمة وأركانها، حسب ما بينها القانون، من دون أن يشوب هذه الإرادة أيّ عيب، يجعل من هذا التصرف غيرَ إرادي.

(أ) العلم.

يتوجب على الجاني، أن يتوفر لديه العلم بكافة عناصر الجريمة، كما حددتها نص المادة (417) من قانون العقوبات الأردني، بحيث يكونُ عالماً، أنّه بممارسته لهذا النشاط، يستخدم وسائل احتيالية مبنية على الكذب والخداع والغش، وأن من شأن هذه الوسائل، إيهام المجني عليه، وحمله على تسليم المال للجاني، بغية تملكه بصورةٍ غيرَ مشروعةٍ لتقع جريمة الاحتيال[2].

---

(1) الشاذلي، جرائم الاعتداء على الأشخاص والأموال، ص513.

(2) صالح، شرح قانون العقوبات القسم الخاص الجرائم الواقعة على الأموال، ص195.

وقد قضت محكمة التمييز الأردنيةفي أحد قراراتها :" إن اتفاق طرفي الوكالة غير قابلة للعزل، المتضمنة عزل الموكل للوكيل، أمر جائز وفقاً لإحكام المادة (241) من القانون المدني، وتعتبر الوكالة منتهية من تاريخ العزل، فإذا قام الوكيل باستعمال صورة عن الوكالة الملغاة، لبيع حصص قطعة الأرض، العائدة للموكل لعدة أشخاص، وانخدع هؤلاء بأنه يملك حق البيع بصفته وكيل، فإن فعله هذا يشكل جرم الاحتيال خلافاً للمادة (417) من قانون العقوبات إذْ يوفر ذلك القصد العام لديه"[1].

كذلك يجب على الجاني، أن يكون عالماً أن المال مملوك للغير، وأنّه ليس له أدنى حق للتصرف به، فشرط العلم مرتبط في نية وقصد الفاعل، فمن غير المتصور، أن يرتكب الشخص جريمة الاحتيال، من خلال طرق احتيالية مبنية على الخداع والغش، والذي لا تولده الصدفة ويدعي بجهله لذلك[2].

(ب) الإرادة.

إن العلم لا يكفي لقيام القصد الجرمي، بل لابد من أن تتجه إرادة الجاني إلى سلوك الطريق الذي جرمه القانون، في الاستيلاء على مال الغير، بإرادة حرة واعية نقية خالية من أي أكراه.

ومن هنا يجب أن يتوافر أمرين أساسيين في إرادة الجاني وهما:

(1) اتجاه إرادة الجاني إلى إتيان وممارسة إحدى صور النشاط الاحتيالي

(2) اتجاه إرادة الجاني إلى تحقيق النتيجة الجرمية بالاستيلاء على المال[3].

ثانياً: القصد الخاص.

ويتمثل في نية تملك الجاني مال الغير، الذي تسلمه من المجني عليه، وحرمانه من مباشرة سلطاته على المال المستولى عليه، بصورة احتيالية، بصرف النظر إذا كان هذا الفعل الاحتيالي قد انقص، أو أضر بالذمة المالية للمجني عليه أم

---

(1) قرار محكمة التمييز الأردنية بصفتها الجزائية رقم 1998/126 (هيئة خماسية) تاريخ 1998/4/29، منشورات مركز عدالة.

(2) بهنام، القسم الخاص في قانون العقوبات، ص532.

(3) أبو خطوة، الجرائم الواقعة على الأموال، ص156.

لا، فمن استولى على مال غيره، وكانت نيته تتجه إلى إعادتــه إليــه، أي لمجــرد مشاهدته، أو من باب المداعبة، فأنه لا يُعد مرتكباً لجريمة الاحتيال، ما دام انتفــت لدية نية التملك، وحتى لا يكون هنالك تشدد وتضيق على سلوك وأفعــال الأفــراد، وبمجرد توافر هذه العناصر المكونة للجريمة، فإنه لا ينظر إلى الباعث لدى الجاني سواء أكان رغبة الجاني هي الانتقام، أو الإضرار بالغير، لأن مالك المال وحده، من يحق له أن يهب أو يتصدق به، فلا تأثير لهذا الباعث مهما كان، ولا أثر له في قيام القصد الجرمي المكون لهذه الجريمة ، ما دام اتجهت نية الجاني إلى تملك مال الغير دون وجه حق له بذلك[1].

ومن بعد تحقق الشروط الواجب توافرها في كل من أركان الجريمــة، مــن الركن المادي والقصد الجرمي، فإن جريمة الاحتيال تخــرج إلــى حيــز الوجــود بصورها المختلفة، وأن المشرع الأردني عاقب على جريمة الاحتيال، فــي نــص المادة (417) في الفقرات الأولى والثانية والثالثة من قانون العقوبات الأردني.

الفقرة الأولى: الحبس من ثلاثة أشهر إلى ثلاثة سنوات، والغرامة المالية من مائة دينار إلى مائتي دينار أردني.

الفقرة الثانية (أ) يعاقب بالحبس مدة لا تقل عن ستة أشهر، إذا ارتكب الفعل بحجة تأمين وظيفة، أو عمل في إدارة عامة.

(ب) يعاقب بالحبس مدة لا تقل عن سنتين، إذا كان مرتكب الجريمة ممن يتولون إصدار الأسهم، أو السندات، أو إي أوراق مالية أخرى متعلقة بشركة، أو مشروع، أو مؤسسة تجارية، أو صناعية.

الفقرة الثالثة: تقضي المحكمة بضعف العقوبة في حال تعدد المجني عليهم.

---

(1) أحمد، الجرائم التي تقع على الأموال في قانون العقوبات الأردني، ص198 وما بعدها. تجدر الإشارة، إلى أن إعطاء شيك بسوء نية، لا يقابله رصيد معد للدفع لا يشكل جريمة احتيال، إنما يشكل جريمة إعطاء شيك بدون رصيد، في حدود المادة (421) من قانون العقوبات،محكمة التمييز الأردنية قرار رقم 1964/112 (هيئة خماسية) تاريخ 1964/8/5 المنشور على الصفحة 921 من عدد مجلة نقابة المحامين بتاريخ 1964/1/1، منشورات مركز عدالة.

وذلك حرصاً من المشرّع على عدم استغلال هؤلاء الأشخاص لمراكزهم الوظيفية، وإن ارتكابهم لهذه الجرائم، يعرضهم لعقوبات أشد منها للمفروضة على غيرهم، كون هذه الفئات من الأشخاص، يتوجب أن تتوفر فيهم الثقة والأمانة وحس المسؤولية لتعاملهم وانخراطهم المباشر مع أفراد المجتمع، الذي يمليه عليهم طبيعة أعمالهم وأنشطتهم المكلفين بالقيام بها(1).

ومن هنا، كان لابد للباحث قبل الدخول في فحوى موضوع الاحتيال الإلكتروني، أن يبين ما هو المقصود بجريمة الاحتيال العادية، ذات الطابع الكلاسيكي المتعارف ع ليها، بمجرد ذكر كلمة احتيال لكي يتسنى للقارئ الفصل بينهما، وأن تأتي كبداية تمهيدية تمكن القارئ من فهم مضمون جرائم الاحتيال الإلكتروني، وكيفية تكوين أركان مثل هذه الجرائم، وما هو الاختلاف بينهما، وأن مصطلح احتيال وحده لا ينصب بالضرورة على استخدا م الطرق الاحتيالية بمفهومها التقليدي، بل لا بد لنا من دخول العالم الافتراضي، والبحث في ثنايا تكنولوجيا المعلومات، لنلامس داء الجريمة، ونضع الخُطة اللازمة لمواجهة هذا الانتشار السلبي للتكنولوجيا، من خلال الضوابط القانونية وبث روح التوعية الضرورية، التي تقع على عاتق البا حثين والمختصين في هذا المجال، والإشارة إلى حجم جرائم الاحتيال الإلكتروني والأسباب الدافعة إلى زيادة هذه الجرائم، كأكثر المخاطر المرافقة لاستخدام الثورة المعلوماتية.

2.1 التعريف بالاحتيال الإلكتروني كأحد الجرائم المعلوماتية:

إن المجتمع الأردني، شأنه شأنباقي المجتمعات المستخدمة للتكنولوجيا، التي باتت جزءً من تعاملات العالم، المنفتح على الصعيد الاقتصادي والاجتماعي، وبما أن الجريمة ملازمة لتطور المجتمعات، فإنّه يتوجب على هذه المجتمعات، أن

---

(1) أحمد، الجرائم التي تقع على الأموال في قانون العقوبات الأردني، ص199. تجدر الإشارة، إلى أن محكمة التمييز الأردنية، أكدت على وجوب الالتزام بعقوبة جريمة الاحتيال، وعدم النزول عن الحد الأدنى في العقوبة، وذلك من خلال قرارها رقم 1997/49 (هيئة خماسية) تاريخ 1997/2/13، منشورات مركز عدالة.



تضع التشريعات اللازمة للحد من ارتكابها، خاصة الجرائم ذات الطابع الإلك   تروني المتطور

فالمشرّع الأردني أصدر العديد من القوانين الناظمة لذلك، مثل قانون المعاملات الإلكترونية رقم (85) لسنة 2001، وقانون البنوك رقم (28) لسنة 2000، وقانون الأوراق المالية رقم (76) لسنة 2002، وإنْ كان تناوله للجريمة الإلكترونية كان بنوع من الاستحياء، إلى أن جاء قانون جرائم أنظمة المعلومات المؤقت رقم (30) لسنة 2010، والذي تناول عدداً من الجرائم المعلوماتية، مثل جرائم الاحتيال الإلكتروني، التي تعد جوهر الجريمة المعلوماتية، وبذلك سد الثغرات التشريعية السابقة للحد من الجرائم الاحتيالية في العالم الافتراضي   ، في محاوله منه لشمول معظم الأفعال غير المشروعة على صعيد تكنولوجيا المعلومات، والحاجة الضرورية للحد من زحف مخاطر هذا النوع من الجرائم.

وعليه سوف نتناول هذا ال قسم، ومن خلال أجزاء متعاقبة نتناول فيها التعريف بالاحتيال الإلكتروني، وحجمه من خلال ال جزء الأول، وسمات مرتكبي جرائم الاحتيال الإلكتروني والأسباب الدافعة لذلك من خلال ال جزء الثاني، وأهم إحصائيات هذه الجرائم والفئات المستهدفة من خلال الجزء الثالث.

1.2.1 التعريف بالاحتيال الإلكتروني وحجمه:

سوف نقسم هذا ال جزء لنتناول التعريف بالاحتيال الإلكتروني، وحجم الاحتيال الإلكتروني.

أولاً: التعريف بالاحتيال الإلكتروني:

إن جرائم الاحتيال الإلكتروني، أو كما يسميه البعض (الاحتيال المعلوماتي)، هي من الجرائم المستحدثة، وقد تعددت التعريفات لهذه الجريمة وإنْ كانت غالبية هذه التعريفات ربطت بين الاستخدام غير المشروع والربح   المادي غير المشروع، في فحوى تحديد مفهوم جرائم الاحتيال الإلكتروني، كقاسم مشترك إلاّ إننا نجدُ عدداً أكثرَ مَن هذه التعريفات للاحتيال الإلكتروني ومن هذه التعريفات أنّه : (كل سلوك احتيالي يتصل بالحاسبات الآلية، حيث تتجهُ نيةُ الفاعلِ إلى تحقيقِ ربح مادي غير

مشروع)[1]، وتم تعريف الاحتيال الإلكتروني على أنّه : (حثُّ الحاسب الآلي على تغيير بعض الحقائق بأي وسيلة كانت تهدف إلى الحصول على ربح غير مشروع على حساب شخص آخر، فوظيفة الحاسب الآلي مكنت الجاني من إتمام فعل الاحتيال)[2]، وهنالك من عرفهُ عُلى أنّه : (كل سلوك احتيالي يرتبط بعملية التحسيب الإلكتروني، بهدف كسب فائدة أو مصلحة مالية)، فقد حيازة ملكية شخص آخر، بقصد الحصول على كسب اقتصادي غير مشروع له، أو لشخص آخر)[3].

وفي إحدى الدراسا ت المسحية، التي قامت بها إحدى الجهات المختصة في الولايات المتحدة الأمريكية، لمحاولة وضـ ع تعريف لمفهوم الاحتيال الإلكتروني، توصلت إلى أنّه من الممكن تعريف الاحتيال الإلكتروني على أنّه (فعل أو مجموعة من الأفعال غير المشروعة، والمتعمدة التي ترتكب بهدف الخداع، أو التحريف للحصول على شيء ذو قيمة، ويكون نظام الحاسوب لازماً لارتكابها)[4].

ومن خلال هذه التعريفات، نلاحظ أنها تباينت في وضع تعريف موحد لجرائم الاحتيال الإلكتروني، يشمل معظم العناصر المكونة للجريمة، وعليه فإنّهُ

---

(1) المومني، نهلا عبدالقادر، (2007)، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر، عمان، الأردن، ص188.

(2) الطوالبة، علي حسن، (2008)، الجرائم الإلكترونية، الطبعة الأولى، جامعة العلوم التطبيقية، البحرين، ص181، 182. مع الإشارة إلى أن قانون المعاملات الإلكترونية الأردني، رقم (85) لسنة 2001، قد عرف بعض المصطلحات المتعلقة بتكنولوجيا المعلومات ونذكر منها:

(أ) الإلكتروني: وهي تقنية استخدام وسائل كهربائية، أو مغناطيسية، أو ضوئية، أو الكترومغناطيسية، أو أيّ وسائل مشابهة في تبادل المعلومات وتخزينها.

(ب) المعلومات: البيانات والنصوص والصور والإشكال والأصوات والرموز وقواعد البيانات وبرامج الحاسوب وما شابه ذلك. أنظر نص المادة الأولى من قانون المعاملات الإلكترونية المؤقت، رقم (85) لسنة 2001.

(3) المومني، الجرائم المعلوماتية، ص189.

(4) الشوابكة، محمد أمين، (2004)، جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، الطبعة الأولى، دار الثقافة للنشر، عمان، الأردن، ص185.

يتوجب أن يكون هنالك مفهوم قانوني شامل، لجرائم الاحتيال الإلكتروني، بحيث يغطي معظم العناصر والأركان المكونة لها، حتى ولو أصبحنا أمام تعريف مطول لمفهوم الاحتيال الإلكتروني، خصوصاً وأن مصطلح الإلكتروني أو المعلوماتي، من المصطلحات المرنة والتي من غير الممكن، أن توصف مثل هذا النوع من الجرائم بعدد محدود من الكلمات، ونحن ما نزال لا نمتلك المعلومات، حول كل المخاطر والأفعال الجرمية المرافقة لتكنولوجيا المعلومات، خصوصاً في مجتمعاتنا العربية حديثة العهد، باستخدام الفضاء الافتراضي الرقمي، الذي يجعل من العالم قريةً صغيرةً في متناول الجميع[1].

ومن خلال ما تقدم من تعريفات، اجتهد أصحابها في نسج مفهوم جرائم الاحتيال الإلكتروني، نجد أنّه من أفضل التعريفات التي تطرقت لمفهوم الاحتيال الإلكتروني والذي يعد أكثر شمولية وقبولا من حيث أنّه حاول أن يجعل كل من الأفعال المؤدية إلى الاستيلاء والتلاعب بأموال وحقوق الغير، فعلاً مجرماً هو تعريف الاحتيال الالكتروني أنّه (التلاعب العمدي بمعلومات وبيانات تمثل قيماً مادية، يختزنها نظام الحاسب الآلي، أو الإدخال غير المسموح به لمعلومات وبيانات صحيحة، أو التلاعب في الأوامر والتعليمات التي تحكم عملية البرمجة، أو أي وسيلة أخرى من شأنها التأثير على الحاسب الآلي، حتى يقوم بعملياته بناءً على هذه البيانات، أو الأوامر، أو التعليمات، من أجل الحصول على ربحٍ غيرِ مشروعٍ وإلحاق ضرر بالغير)[2]، ويرى الباحث أن هذا التعريف لامس جوهر مفهوم جرائم الاحتيال الإلكتروني، على أنّه يشمل التلاعب بالبيانات والإدخال والتحكم بالبرمجة ونظام التخزين الآلي؛ بغية الحصول على الربح المادي غير المشروع، والإضرار بالغير محاولاً أن يشمل العناصر المكونة لجريمة الاحتيال الإلكتروني، والتي تعد

---

(1) كريدلي، نهاد، (2011)، الجريمة والاحتيال في البيئة الإلكترونية، متوفر عبر الموقع: http://www.nasbcom.net/vb/showthread.php، 3/9/2011

(2) قورة، نائله، (2005)، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، القاهرة، مصر، ص424، 425.



من الجرائم حديثة العهد، التي تقع في العالم الافتراضي متجاوزة الحدود الـسياسية والمجتمعات، والقائمة بدورها على الابتكار والتجديد.

هذا ونلاحظ تطور في تحديد وتعريف مفهوم جرائم الاحتيال الإلكترونـي، ليتماشى مع الطبيعة التشريعية، بما يناسب تطور الحيـاة واسـتخدام المجتمعـات لتكنولوجيا المعلومات، بالشكل السليم والأكثر أمناً،فمع مرور الوقت، وكنتيجة حتمية لاتساع استخدام الثورة المعلوماتية، نجد في كل من هذه الجزئيات فـي التعريـف السابق، قد يـ تشكل منه عدد من الجرائم بمنظور أكثر تطوراً، خصوصاً أن ارتبـاط تجريم الأفعال من خلال استخدام التكنولوجيا بات مرتبطـاً بمقـدار هـذا التطـور المستمر، والذي يتمخض عن الكثير من المخاطر، التي تـستهدف أمـن المجتمـع وحقوق الأفراد[1] وهو يتفق معه الباحث لأن مثل هذا التعـ ريف استخدم أكبر قدر ممكن من المصطلحات لتوفير أكبر قدر من الحماية.

ثانياً: حجم الاحتيال الإلكتروني

من الصعوبة بمكان، حصر مثل هذا النوع من الجرائم بأرقام ونسب، ومـع ذلك نجد أن الإحصائيات التي تصدر عن الجهات المختصة، في الكثير من الـدول تحتوي على تحفظات كثيرة من حيث النسب الحقيقية، إلا أنّها في الغالب ما تكـون مبالغ مالية كبيره قد تضر بالاقتصاد الوطني، مما يؤدي إلى هز ثقة الاستثمار فيها سواءً على الصعيد الداخلي، أو في التعاملات التجارية لها[2].

نجد مجلة لوس انجلوس تايمز في عددها الصادر فـي 22 مـارس لـسنة 2000 ذكرت أن خسارة الشركات الأميركية لوحـدها، جـراء جـرائم الاحتيـال الإلكتروني بلغت حوالي 10 مليار دولار سنوياً بواقع 68%، من قبـل أشـخاص يعملون داخل هذه المؤسسات والشركات و 32% هم من خارج هذه المؤسسات[3].

---

(1) المكاوي، محمد محمود، (2010)، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية، الطبعة الأولى، المكتبة العصرية للنشر، القاهرة، مصر، ص321.

(2) يوسف، أمير فرج، (2008)، الجرائم المعلوماتية على شبكة الانترنت، الطبعة الأولى، دار المطبوعات الجامعية للنشر، الإسكندرية، مصر، ص51.

(3) http://www.nasbcom.net/vb/showthread.php?t=7558&page=1.

وأظهر مسح أُجري من قبل معهد أمن الحاسوب الأمريكي) في عام (1999م)، أنّ خسائر (163) مئة وثلاثة وستون شركة أمريكية، من الجرائم المتعلقة بالحاسب الآلي، بلغت أكثر من (123) مئة وثلاثة وعشرين مليون دولار أمريكي، في حين أظهر المسح الذي أُجري في عام (2000) ارتفاع عدد الشركات الأمريكية المتضررة من تلك الجرائم، حيث وصل إلى (273) مائتين وثلاث وسبعين شركة، بلغ مجموع خسائرها أكثر من (256) مائتين وستة وخمسون مليون دولار ومن الملاحظ أن جرائم الاحتيال الإلكتروني، ونتيجة التطور المصاحب للمجتمعات الغربية والأوروبية، فإن لمثل هذا النوع من الجرائم تاريخ جاب هذه البلدان من بداية الثمانينيات[(1)]،خصوصاً أنّه من العام 1981 الذي شهد تصنيع وإنتاج الكمبيوتر الشخصي ذو الحجم الصغير، وسهل الاستخدام مقارنة عما كان عليه الحال قبل ذلك، إذ كانت أجهزة الكمبيوتر، كبيرة ومعقدة وثابتة وغير متوفرة في أيدي معظم الفئات من الأفراد، إذ كانت مقتصرة على كبرى المؤسسات والجهات الحكومية، ومع مرور الوقت، وازدياد انتشار هذه التكنولوجيا، أدت إلى تطور هذه الجرائم بمطلع التسعينيات، لتعلن الثورة الحقيقية، وذلك لانتشار تكنولوجيا المعلومات بشكل غير مسبوق على الصعيد العالمي، واعتراف الدول بحجم هذه الظاهرة، التي باتت خطراً حقيقياً يمس أمن المجتمعات والدول والأفراد على حداً سواء[(2)].

أما على الصعيد العربي، فلم يعد المجتمع آمناً من جرائم الاحتيال الإلكتروني، وأن تفاوتت النسب بين مجتمعاتها التي تعتبر من دول العالم الثالث والدول النامية، سيما تلك الدول التي أخذت بمشروع الحكومة الإلكترونية ومحاولة صقل موظفيها صبغة العمل الإلكتروني، مثل دولة الإمارات العربية المتحدة التي سارت على هذا النهج لكثرة وانتشار استخدام تكنولوجيا المعلومات فيها، وهذا هو

---

(1) منشاوي، محمد عبدالله، (2011)، جرائم الانترنت من منظور شرعي وقانوني، متوفر عبر الموقع: http://www.dahsha.com/old/viewarticle.php?id=32327.

(2) المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية، ص322.

الشأن نفسه الذي تسعى إليه الحكومة الأردنية فيما يسمى بالحكومة الإلكترونية، وأن مصر وبحكم عدد سكانها وانتشار التعاملات الإلكترونية فيها نالت جانباً من جـــرائم الاحتيال الإلكتروني، وفي العام 2000 فلقد تم القبض على عصابة مــن مجرمــي الاحتيال الإلكتروني، وهم من طلبة الجامعات، عندما قامو ا بالاستيلاء على حسابات الفيزا كارد الخاصة ببعض العملاء، والتابعة لعددمن البنوك المــصرية [1]، فمــن الملاحظ أن حجم هذا النوع من الجرائم بات في تزايد قائماً علىً الابتكار، غير آبــه بما يسمى حدود دولية، وأخذ من الفضاء الافتراضي بيئة ومناخ مناسباً ومنافساً في منظومة الجريمة المعلوماتية[2]، وإن كنا نلاحظ انتشار هذه الجــرائم، فــي الــدول الغربية أقدم تاريخياً، ألا أن خطر هذه الجرائم يدق أبواب دول العالم الثالث بــشكل كبير، في ظل الضعف التشريعي، وحداثة مثل هذه الجرائم على صعيد المنظومــة التشريعية أو النسق الاجتماعي، وهنا لابد من بث التوعية اللازمة وانخراط الباحثين وأصحاب الاختصاص في البيئة العم لية، للحد من انتشار هــذه الجــرائم، ووضــع الإستراتيجية الواضحة بين المؤسسات وأصحاب الشركات، والبنوك بالتعــاون مــع الجهات الأمنية[3].

2.2.1 سمات مرتكبي جرائم الاحتيال الإلكتروني والأسباب الدافعة لارتكابها

سوف نتناول سمات مرتكبي جرائم الاحتيال الإلكتروني، ونتنــاول دوافــع مرتكبي جرائم الاحتيال الإلكتروني.

أولاً: سمات مرتكبي جرائم الاحتيال الإلكتروني

إن الاحتيال الإلكتروني، لا يبتعد عن الجرائم المعلوماتية من حيث الصفات العامة لمرتكبيها، وإنْ كانت غير ثابتة، بوجود بعض الفوارق مع الإشارة إلــى أن جرائم الاحتيال الإلكتروني ، قد تقع من قبل العاملين بالمؤسسات المجني عليهــا، أو

---

(1) سلامة، عماد، (2005)، الحماية القانونية لبرامج الحاسب الآلي ومشكلة قرصنة البرامج، الطبعة الأولى، دار وائل للنشر، عمان، لبنان، ص36 وما بعدها.

(2) العريان، محمد علي، (2004)، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، ص22.

(3) سلامة، الحماية القانونية لبرامج الحاسب الآلي ومشكلة قرصنة البرامج، ص40.

من خلال أشخاص من خارج هذه المؤسسات، وتقع من قبل أشخاص مصرح لهم بالدخول والتعامل مع أجهزة الحاسب الآلي، وممن هم غير مصرح إليهم، وقد نكون أمام عُلاقة وثيقة بين الجاني والمجني عليه [1]، أو لا تكون أدنى معرفة بينهم فنحن نتعامل مع عالم افتراضي يتوجب على كل من ارتضى إلى نفسه، ولوجَ هذا الفضاء الرقمي، أن يتخذ الاحتياطات اللازمة لذلك، وفي الغالب أن معظم مرتكبي هذه الجرائم هم من العاملين بالمؤسسات المجني عليها، وممن مصرح لهم بالدخول ومعالجة البيانات[2]، ففي دراسة أُجريتْ في المانيا، تبين أن ما نسبته 90% من حالات الاحتيال الإلكتروني، وقعت من قبل العاملين داخل المؤسسات المجني عليها من خلال التلاعب في إدخال البيانات والمعلومات، أو في مرحلة الإخراج، أو مرحلة التعامل معها بعد تخزينها في أجهزة الحاسب الآلي، ونتيجة للتطور الملحوظ والسرعة في انتشار نظم الحاسب الآلي عن بعد(Remote Access) نجد أن النتائج في طور التغيير، إذْ سوف تزداد نسبة ارتكاب جرائم الاحتيال الإلكتروني، من قبل الأشخاص غير العاملين بالمؤسسات، سيما أنها باتت لا تتطلب التقنية العالية لإرتكابها من قبل الأفراد العاديين المختصين وغير المختصين، فالأمر بات طبيعياً لا بل أصبح من ضروريات الحياة العلمية، والعملية، والابتعاد عن ممارسه هذا التطور، ومواكبته قد يؤدي إلى عزلة هؤلاء المتهجسين من تكنولوجيا المعلومات، وتفويت حتى فرص العمل والتعامل، والتواصل مع الآخرين، خصوصاً فئة الشباب الذي بات إلمامه بهذه الثورة المعلوماتية، أمر واجب قد تتوقف عليه مسيرة عمله بالمجتمع الرقمي الجديد[3].

فالسمات العامة المفترضة لمرتكبي جرائم الاحتيال الإلكتروني والسمات المشتركة بينهم تتمثل فيما يأتي:

---

(1) أحمد، مؤمن، (2005)، أمن الانترنت المخاطر والتحديات، مكتب نائب رئيس مجلس الوزراء لشؤون الإعلام، أبو ظبي، الإمارات، ص33 وما بعدها.

(2) المحمدي، حسنين، (2008)، إرهاب الانترنت الخطر القادم، الطبعة الأولى، دار الفكر الجامعي للنشر، الإسكندرية، مصر، ص51.

(3) قورة، جرائم الحاسب الآلي الاقتصادية، ص225 وما بعدها.

(1) أن نسبة الذكور هي الأكبر مقارنة مع الإنـاث ممـن يرتكبـون الجـرائم الاحتيالية بصورة عامة؛ وذلك بسبب التفوق العددي للـذكور فـي مجـال استخدام تكنولوجيا المعلومات، والحاسبات منها لدى الإناث[1].

(2) تبدل القيم الأخلاقية لديهم بوجه عام، خصوصاً أنهـم يبـررو ن أفعـالهم الجرمية ذاتياً؛ مما يبعدهم عن دائرة الشك إلى حد كبير، وإحساسهم بالرضا عن هذه الأفعال التجريمية، والتي ينظـرون إليهـا بنـوع مـن الإباحيـة والحريات، سيما أنهم ليسوا من أصحاب السوابق الإجرامية[2].

(3) غالبيتهم من صغار السن وفئة الشباب، والتي تتراوح أعمارهم بين 18 و35 عام وإن كان ذلك لا يمنع أن ترتكب هذه الجرائم من كبار السن وإنْ كانـت بنسب قليلة مقارنه مع فئة الشباب، والتي في الغالب ما يُمكنّها هذا السن من المكوث مدة اطول في استخدام أجهزة الحاسب الآلـي وشـبكة الانترنـت، الفضاء الرحب لجرائم الاحتيال الإلكتروني، خصوصاً مع قلة تكلفـة هـذه التقنية[3].

(4) يتميز غالبية مرتكبي جرائم الا حتيال الإلكتروني، بعدم وجود سوابق إجرامية بسجلاتهم، وفي العادة يكونون ممن يتولون المناصب في المؤسسات المجني عليها، والتي تتطلب الثقة وحس المسؤولية من قبل الإدارة وأصحاب هـذه المؤسسات، وهذا ما يخرجهم من دائرة الشك وصعوبة القبض على مثل هذه الفئة المستترة بمظلة السلطة وحسن السلوك المفترض[4].

(5) عدم تميز أكثرهم بالتقنية العالية، فالغالبية يكتشفون الثغرات في هذا الحاسب الآلي، نتيجة استعمالهم المتكرر والمتواصل، واصحاب الاختـصاص فـي

---

(1) سلامة، الحماية القانونية لبرامج الحاسب الآلي ومشكلة قرصنة البرامج، ص44.

(2) المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية، ص320.

(3) نبيه، نسرين عبدالحميد، (2008)، الجريمة المعلوماتية والمجرم المعلوماتي، دار المعارف للنشر، الإسكندرية، مصر، ص23.

(4) قورة، جرائم الحاسب الآلي الاقتصادية، ص226 وما بعدها.

تكنولوجيا المعلومات لا يشكلون إلا فئة بسيطة، وإنْ كانت هذه الفئة أشد خطورةً من غيرها، هذا وإن نسبة المتخصصين والمحترفين في المجال الإلكتروني في تزايد ملحوظ، مما يوصلنا إلى ازدياد حجم مخاطر هذه الجرائم بشكلٍ أكثرَ مما هو عليه[1].

ثانياً: دوافع مرتكبي جرائم الاحتيال الإلكتروني

سوف نبين بعض الدوافع الأكثر شيوعاً بين مرتكبي مثل هذا النوع من الجرائم[2]:

(1)الفراغ والتسلية مع الآخرين : أن بعض مرتكبي جرائم الاحتيال الإلكتروني قد يكون الدافع لديهم التسلية مع الآخرين، وملئ الفراغ، وسرعان ما تتطور الأمور داخل المكنون الذاتي لذلك الشخص، ليضع نصب عينه مقدرته الانسياق في ارتكاب جرائم الاحتيال الإلكتروني ، وما يلبث إلا أن بات ينتهك القوانين الناظمة لحقوق الإفراد، ومرتكب لجرائم الاحتيال الإلكتروني، ومانح نفسه الثقة بعدم مقدرة الآخرين من اكتشاف أمره.

(2) إثبات قدرته على الاختراق للحاسبات الإلية، أو بدافع الفضول واكتساب الخبرة،حيث تتبلور لدى هذا الشخص مقدرته على الولوج إلى أنظمة الحاسبات الآلية، والتفاخر بنفسه مع اقرانه لاسيما فئة المراهقين والشباب، وتعزيز قدراته واكتساب الخبرة اللازمة للتعامل مع هذا العالم الافتراضي، فيقحم نفسه بجرائم الاحتيال الإلكتروني ناسباً الذكاء لذاته، وهذا من الدوافع الأكثر انتشاراً في الدول الأوروبية والولايات المتحدة الأمريكية، وما يتفق

(1) Shipley, T. & Hutchings, C., (2010) , Report on Cyber Crime investigation, A Report of the International High Tech Crime investigation Association, p:4.
تجدر الإشارة، إلى أن هذه السمات المشتركة، بيت مرتكبي هذه الجرائم، هي غير ثابتة، ومتغيره بحسب ما يطرأ على هذه الجرائم، من تطور، وإنها تختلف من بلد إلى آخر، خصوصاً في المجتمعات العربية، والتي تعكس واقع النمط المعيشي لهذه المجتمعات، بين مرتكبي هذا النوع من الجرائم. أنظر ذلك من خلال. أحمد، أمن الانترنت المخاطر والتحديات، ص40.

(2) نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، ص26.



وطبيعة المجتمع بتلك البلدان كونها من أوائل الدول المستخدمة لتكنولوجيا المعلومات ومن يساهم بتطورها[1].

(3) تحقيق الربح المادي غير المشروع، وأن كانت أشد خطورة عندما ترتكب من قبل الجماعات المنظمة ذات الـ دراية بالأنظمة الرقمية للحاسبات الآلية وثغراتها، متسلحة بهذه المهارة مستخدمين الطرق الاحتيالية، للاستيلاء على مال الغير دون وجه حق، وهو الدافع الأكبر لارتكاب جرائم الاحتيال الإلكتروني[2].

(4) إلحاق الإضرار بالمجني عليه بدافع الحقد والغيرة، دون أن يكون الباعث الكسب المادي، والذي بالعادة يتحقق بإتمام الجريمة، فالإضرار نتيجة حتمية من آثار الاحتيال الإلكتروني، وغالباً ما تقع بين الشباب المقيمين داخل الدولة الواحدة[3].

(5) معاناة الجاني من مشاكل مادية وصعوبات من تحقيق أرباح مادية، بالإضافة إلى عدم مقدرته على ارتكاب جرائم تقليدية، بمواجهة محتملة مع المجني عليه، خصوصاً أنّه يتولد لديه قناعة بأن المؤسسات المجني عليها، لن تتأثر بما يقدم عليه، وأنها قادرة على تحمّل هذه الخسائر، أكثر منها لدى الأفراد، والحفاظ على سمعتها وعلاقاتها مع المتعاملين معها سوف يجعلها تتستر على الحادثة أكثر منها، محاولة اللجوء إلى السلطات المختصة، وأن مثل هذا النوع من الجرائم يعتبر غطاءً له ولا يحتاج إلى الوقت، الذي تتطلبه الجرائم التقليدية الأخرى[4].

---

(1) قورة، جرائم الحاسب الآلي الاقتصادية، ص427.

(2) الفيل، علي عدنان، (2011)، الإجرام الإلكتروني، الطبعة الأولى، منشورات زين الحقوقية، بيروت، لبنان، ص61.

(3) أحمد، أمن الانترنت المخاطر والتحديات، ص37 وما بعدها.

(4) آل عدينان، عبدالله محمد، (2011)، الاحتيال المعلوماتي، مركز التميز لأمن المعلومات، متوفر عبر الموقع: www.coeia.edu.sa.

(6) دوافع وبواعث سياسية تجول في مخيلة الجاني، خصوصاً عند استهداف المؤسسات ذات المراكز السيادية، للإختلاف بالنهج السياسي، فيعهد إلى نفسه محاولة الإضرار بها، والربح المادي غير المشروع، وذلك انطلاقاً من إيمانه بأفكاره، والنظر إلى كل من يخالفه هذا النهج السياسي المرسوم بمخيلته، يعتبره عدو له يبرره داخلياً بممارسة هذه الإعمال، التي يريدها إسوةً بغيره من أصحاب القرار[1].

(7) الإهمال وضعف الرقابة، وتعد هذه من أهم الدوافع والبواعث التي يجب التصدي لها، على الصعيد الاجتماعي والتشريعي، والذي يتمثل بإساءة استخدام الحاسب الآلي بصورة غير مشروعة، والدافع لارتكاب جرائم الاحتيال الإلكتروني، وفي كثير من الأحيان، سُرعانٌ ما يؤدي الإهمال إلى ارتكاب جرائم تتعدى جرائم الاحتيال الإلكتروني، قد تصل حد إزهاق الأرواح، وكل الأعمال التي تصنف تحت دائرة التجريم القانوني والأدبي[2].

ونجد أن الدوافع قد تتسم بالعمومية، لكثير من مجالات الحياة، وأن المجتمع المسؤول الأول عن كثير من هذه الدوافع، التي تعكس المناخ الآمن والسليم لاستخدام تكنولوجيا المعلومات، من خلال تعاونه مع الجهات الرقابية، والأمنية بالصورة الفاعلة التي تحد من انتشار هذه الجرائم، والتي تسهم في استخدام أمثل وآمن لتكنولوجيا المعلومات، على الصعيد المحلي والعالمي، وأن كنا سوف نتحدث عن الجهود الدولية والإقليمية، بشكل أكثر تفصيل في نهاية الفصل الثاني، من موضوع هذا البحث، ومن خلال ما تطرقنا له من دوافع مرتكبي جرائم الاحتيال الإلكتروني، يجب الإقرار أن هنالك من الأسباب، ما تساعد وتسهم بشكل أو بآخر، على انتشار جرائم الاحتيال الإلكتروني نحاول إجمالها فيما يلي[3]:

---

(1) عبابنة، محمود، (2004)، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر، عمان، الأردن، ص56.

(2) حجازي، عبدالفتاح بيومي، (2009)، علم الجريمة والمجرم المعلوماتي، الطبعة الأولى، دار المعارف للنشر، الإسكندرية، مصر، ص105 وما بعدها.

(3) العريان، الجرائم المعلوماتية، ص21.

(1) غياب المراجعة الدورية للمعلومات المخزنة، بعد إدخالها إلى جهاز الحاسب الآلي، مما يساعد الجاني إلى الولوج والتلاعب بالبيانات، وارتكاب الجريمة، وعدم اكتشافها إلا بعد مضي مده طويلة من ارتكابها، وهذا يُضعف من فرصة إلقاء القبض على الجاني المحتال، وتجعل من ذلك حافزاً لديه لتكرار ارتكاب الجريمة، خلال مدة اقصر على اعتبار علمه بضعف الإشراف الوقائي[1].

(2) الاعتماد بشكل كبير وأساسي، على أجهزة الحاسب الآلي فيما يتعلق بالتعاملات التجارية، وتحويل الأموال، والشراء عبر الانترنت، وتهافت العروض من خلال هذه الشبكة العنكبوتية، خصوصاً بالصفقات والتحويلات المالية الكبيرة، والتي من المستحيل أجرائها بدون استخدام المنظومة الإلكترونية، التي تعتبر الملاذ الوحيد في توفير السرعة والدقة في انجاز المعاملات، مقارنةً بما كانت عليه الأمور[2].

(3) أن معظم الملفات المحتوية على البيانات والمعلومات، تخزن داخل الحاسب الآلي، دون ظهورها بشكل مباشر على شاشة الجهاز (سطح المكتب)، إلا إذا أُعطي الجهاز أمراً بذلك، وهذا ما يساعد أيضاً على عدم اكتشاف جريمة الاحتيال، ما لم يتم المتابعة الدورية، وإلا ظلت الجريمة في طي النسيان، ما لم تلعب الصدفة دورها في ذلك، ونبقى ندور في عالم اللامنهجية في كيفيه استخدام مثل هذا التطور بما يتناسب وإمكانياتنا[3].

(4) عدم كفاية الإجراءات الأمنية اللازمة، لمجاراة التطور التكنولوجي المرتبط بالحاسب الآلي، وعدم أخذ مفهوم الأمن المعلوماتي، والتكنولوجي على محمل الجد، والنظر إلى الأمر وكأننا في منئى عن مخاطر مثل هذه الجرائم، والتي تعتبر أمر واقعي وضريبة ثمرة هذا التقدم العلمي، على كافة الأصعدة والمستويات.

---

(1) أبو شامة، عباس، (2008)، عولمة الجريمة الاقتصادية، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، ص50.

(2) حجازي، علم الجريمة والمجرم المعلوماتي، ص106.

(3) قورة، جرائم الحاسب الآلي الاقتصادية، ص431 وما بعدها.

(5) منح الثقة من قبل إدارة المؤسسات، إلى موظفيها الذين يشكلون النسبة الأكبر من جناة الاحتيال الإلكتروني، بشكل غير متوازن، وحجم الرقابة الإدارية عليهم، مما يدفع إلى زيادة ارتكاب جرائم الاحتيال الإلكتروني، وبشكل أكثر تنظيماً، ما دام إن مثل هذه الثقة لا يقابلها وزن مماثل من الرقابة على أقل تحديد[1].

3.2.1 أهم الإحصائيات الخاصة بجرائم الاحتيال الإلكتروني والفئات المستهدفة بها

إن جرائم الاحتيال الإلكتروني، المبنية على الغش والخداع، دائما ما يكون فيها للمجني عليه دوراً بارزاً في تسهيل مهمة الجاني، من خلال التعاون معه والمتمثل بالانسياق وراء أكاذيبه، وذلك بحسب واختلاف الشخصية التي يتمتع بها كل من ضحايا الاحتيال، فقد نجد الضحايا من أصحاب المستوى التعليمي العالي، ومع ذلك يقعوا في شراك الجاني، من دون أن تشفع لهم هذه المكانة، ومنهم من ينتمي للمستويات المنخفضة في وعيهم ودرجاتهم العلمية، ونجد فئة قد تتوسط هؤلاء، ولكن ليس لديها القدر الكافي للحرص في تعاملاتها مع الآخرين، أو كما يطلق عليهم البعض أصحاب النوايا الحسنة، الذين يتهاونون في استرجاع حقوقهم خجلاً وحياءً[2].

ومن خلال عدد من الدراسات، التي أُجريت في الولايات المتحدة الأميركية، ومقارنة بالمجتمعات العربية، نجد أن الاحتيال الإلكتروني، الذي يتولد نتيجة الطمع والرغبة في الاستيلاء على الأموال في القطاع المالي والشركات، تحتل المرتبة الأولى بين الكثير من الولايات، ونذكر بعض هذه النسب لهذا القطاع من خلال دراسة أُجريت في العام 2000 لعدد من الولايات ومنها: ولاية كاليفورنيا حيث بلغت نسبة الاحتيال الإلكتروني نتيجة هذا الطمع بالمال 17,3%، ولاية فلوريدا 8,1%، ولاية نيويورك 7,7% ولاية تكساس 5,1 % وذلك بطبيعة الحال، نتيجة للقوة

(1) أحمد، أمن الانترنت المخاطر والتحديات، ص38.
(2) Internet Fraud Complaint Center (IFCC) , (2001) , Six-Month Data Trends Report, National White Collar Crime Center and the Federal Bureau of Investigation.p 6.

الاقتصادية وحجم الأموال المتداولة في مثل هذه البلدان، وكيفية تفاوتها أيضاً فيما بينها داخل البلد الواحد، في إشارة إلى أن هذا النوع من الجرائم بات مرتبط بصورة أو بأخرى بالمجتمعات ذات البنية الاقتصادية المتطورة، وأنه يتماشى وسلوك واهتمامات هذه المجتمعات [1]، وفي السياق ذاته، وفي دراسة أجرتها شركة مكافي لتكنولوجيا المعلومات في نهاية العام 2009، أن الشركات الأوروبية، تتكبد خسائر تقدر بتريليون دولار سنوياً، علًى رأسها جرائم الاحتيال الإلكتروني، وفي دراسة أجرتها شركة "أرك سايت" الأمريكية الأمنية، ومؤسسة أبحاث تكنولوجيا المعلومات بمعهد" بونيمون" الأمريكي، تشير إلى تكبد الشركات الأميركية خسائر تقدر بحوالي 8.3 مليون دولار سنوياً، نتيجة الجرائم الالكترونية 22% نسبة جرائم الاحتيال الإلكتروني، كما كشفت السلطات الأميركية في نهاية العام 2009، أن أكثر من 130 مليون بطاقة ائتمان وبطاقة سحب مصرفية، تم الاستيلاء عليها بطرق احتيالية وقرصنه الكترونية، ومن خلال دراسة، قامت بها شركة نورتن الرائدة في مجال تطوير الحلول البرمجية الأمنية، أن ثُلثي مستخدمي الانترنت حول العالم، تعرضوا لجريمة الكترونية على الأقل مرة واحده، تمثلت في هجمات فيروسية، وعمليات احتيالية للاستيلاء على بطاقات الائتمان والبيانات المصرفية الشخصية[2].

وفي أخر دراسة، قامت بها شركة نورتن بالتعاون مع شركة " ستراتيجي ون" في 42دولة، من ضمنها دولة الإمارات العربية المتحدة، في مطلع العام 2011، والتي تشير إلى أن أكثر من 1,4 مليون مستخدم للانترنت في الأمارات، يتعرضون لهجمات الكترونية يومياً، حيث بلغت نسبة جرائم الرسائل الاحتيالية 19% ومحاولة الاستيلاء على المعلومات المصرفية 18%وقدرت هذه الخسائر بنحو 209مليون دولار سنوياً، وأن نسبة الجرائم الإلكترونية، التي يتعرض لها مستخدمي الانترنت تفوق بكثير نسبة الجرائم العادية، بنسبة تتجاوز 32% من معدل ارتكاب الجريمة.

---

(1) العسبلي، منى شاكر، (د.ث)، تأثير الجريمة الإلكترونية على النواحي الاقتصادية، متوفر عبر الموقع: www.coeia.edu.sa.

(2) http://www.itp.net/arabic/586177، p1 of 2, date21/1/2012

وتشير الدراسات أن من أهم صور جرائم الاحتيال الإلكتروني، الأكثر انتشاراً في المجتمعات العربية ما يلي:

(1) الاحتيال على الأفراد:

كما هو الاحتيال قائم على الغش والخداع، فإن الأفراد سواء أكانوا رجال أعمال أو أفراد عاديين أو هواة وغيرهم، فالعبث بمخيلة الضحية، يكون مفتاح التلاعب والخداع الذي يسعى إليه الجاني من نافذة الأفراد، من أجل تحقيق الربح المادي غير المشروع على حسابهم، وتختلف الأنماط الإجرامية على الأفراد ونذكر منها على سبيل المثال:

(أ) الاحتيال من خلال الإعلان، عن تنظيم لمسابقات وهمية على شبكة الانترنت والمواقع التفاعلية الإجتماعية، بهدف الإستيلاء على أموال الأفراد، مستخدمين عامل الإغراء بالفوزبجوائز مغرية مقارنة بما يدفعه المتسابق (الضحية) من مبلغ بسيط[1].

(ب) الاحتيال على الأفراد الراغبين بالسفر، للعمل بالدول العربية والأوروبية، والادعاء بإمكانية تأمين العمل لهم، مقابل مبالغ يتم تحويلها من قبل الأفراد، دون التأكد من أي وجود للجناة، معتمدين فقط على المراسلات الإلكترونية الخادعة، وخاصةً في الدول ذات التعداد السكاني الكبير، في كل من قارة أسيا، وإفريقيا، والدول التي تعتبر مصدّره للأيدي العاملة، مثل مصر، اندونيسيا، نيجيريا، وغيرها من الدول التي يسعى الكثير من أفرادها لا بل يحلمون بالسفر للعمل خارج بلدانهم[2].

(ج) الاحتيال من خلال الإعلان، عن تأمين رحلات العمرة والحج، مستخدمين أوقات الحج ونبل الغاية من السفر، والعمل على الجانب العقائدي بطرق

---

(1) الشناوي، محمد، (2007)، جرائم النصب المستحدثة، دار شتات للنشر، القاهرة، مصر، ص71.

(2) يوسف، الجرائم المعلوماتية على شبكة الانترنت، ص78.

احتيالية[1]، تبين مدى تجرد هؤلاء الجناة المحتالين، من أدنى مقومات الإحساس البشري، للكسب غير المشروع من خلال إعلانات ومواقع لا أساس لها من الصحة، سوى أنها مواقع وهمية على الانترنت.

(د) الاحتيال من خلال رسائل الهاتف المحمول، والتي باتت ظاهرة آخذه بالانتشار، وذلك لكثرة المستخدمين مثل مصر، والأردن، ودول الخليج العربي، وإرسال هذه الرسائل إلى أكبر عدد ممكن من الأفراد، واقتطاع مبالغ على مسابقات وهمية، من خلال مزودات خدمة معده لهذه الغاية[2].

(2) الاحتيال على الشركات

إنّ كثير من الشركات، تكون محط أنظار جناة الاحتيال الإلكتروني، وذلك من أجل الحصول على أرباح مادية غير مشروعة، بأرقام أكثر منها لدى الأفراد، واعتقادهم بمقدرة الشركات سيما الكبرى منها، على تحمل الخسائر، وتخوف هذه الشركات، من الإبلاغ عن مثل هذه الجرائم الاحتيالية المرتكبة في حقها، حفاظاً منها على السمعة وعلى ثقة العملاء، سوا على الصعيد الداخلي أو الخارجي، وقد يأتي الاحتيال على الشركات، إما بشكل فردي من قبل الأفراد، أو من خلال جماعات منظمة، أو من خلال شركات أخرى، غالباً ما تكون شركات وهمية وغير مشروعة، تعمل كستار لعملياتها الاحتيالية، وأن كثير من الشركات العالمية سيما الغربية منها، غالباً ما تكون محط أنظار الجناة، ففي كندا قام احد المحتالين عام 2002 بشراء 6550سهم من إحدى الشركات، بعد أن تلاعب بالأوراق المالية الخاصة بها، وقام ببيعها بربح وصل لغاية 17000 الف دولار، ليتم بعد ذلك اكتشاف الأمر وتقديم المحتال إلى القضاء، في حين ينتشر مثل هذا النوع من الاحتيال على الشركات، من خلال التلاعب بشراء وسمسرة الأسهم في كل من الولايات المتحدة الأمريكية،

(1) مصطفى، أحمد، (2010)، جرائم الحاسبات الآلية في التشريع المصري، الطبعة الأولى، دار النهضة للنشر، الإسكندرية، مصر، ص24.

(2) المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية، ص122.

واستراليا، بالإضافة إلى كندا [1]، ومن أهم الأنماط والصور المستخدمة في مجال الاحتيال الإلكتروني على الشركات، نذكر أهم هذه الصور على سبيل المثال على النحو الآتي:

(أ) إنشاء شركات وهمية مساهمة، بموجب سندات غير صحيحة، واستخدامها للاحتيال على الأ فراد والشركات، من خلال طرح أسهم للاكتتاب، والتداول، والاستيلاء على القيمة المالية لهذه الأسهم، والتي هي بالأصل لم تتخذ الصفة الرسمية، خصوصا أن كثير من هذه التعاملات، باتت تستخدم الكترونياً، ومستغلة ميزة السرعة والسهولة في إتمام مثل هذه الصفقات[2].

(ب) الادعاء بتنظيم حفلات خيرية باسم منتديات، أو ملتقيات وجمعيات خيرية، والترويج لها الكترونياً، وجمع التبرعات، وتذاكر الحفل قبل الموعد المزعوم للحفل، من خلال أرقام حسابات يتم الإعلان عنها، وسرعان ما تحول هذه المبالغ إلى حسابات سريه من الصعب التوصل إليها، وأنّه لا ّ وجود لأي جهة راعية، وليس هنالك مكان محدد لما تم الترويج إليه، وكل ما في الأمر، هو الترويج الكترونياً لهذا الحفل بصورة وهمية، ومحاولة للاستيلاء على المال، بصورة غير مشروعة من ثم الاختفاء عن الأنظار[3].

(ج) القيام باستهداف الشركات، من خلال استغلالها للإعلان عن مسابقات وهمية، بهدف جمع مبالغ مالية من المشاركين، دون وجود للمسابقة الحقيقية، أو تراخيص لازمة لممارسة هذا النشاط، الذي في ظاهره مشروع وباطنه احتيالي، وخصوصاً الشركات المختصة بهذا النوع من الترويج الإعلاني، من خلال المواقع الإلكترونية الأكثر انتشاراً، وً مصداقية وقبول لدى الأفراد والمتعاملين بها، وكما هي متنوعة أساليب الاحتيال الإلكتروني، ولكن القاسم

(1) Graycar, A. & Smith, R., (2002) , Identifying and Responding to Electronic Fraud Risks, 30th Australasian Registrars Conference Canberra.p.5.

(2) المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية، ص123.

(3) الغثبر، خالد بن سليمان؛ والقحطاني، محمد بن عبدالله، (2009)، أمن المعلومات، الطبعة الأولى، جامعة الملك سعود، الرياض، السعودية.

المشترك فيها، عدم وجود مقابله أو أي اجتماع بين الجاني والضحية [1]، حيث يقوم الجاني المحتال بعدد من المخاطبات مع إدارة هذه الشركات، من دون أن يجتمعا مع بعض، فالجاني همة أن يبقى بعيداً عن الأنظار، ويجعل من العالم الافتراضي، مسرحاً لأفعاله الاحتيالية، وسرعة في انجاز هذه المهام الاحتيالية، والذي دائماً ما يزود نفسه بالشجاعة والثقة المفرطة.

من بعض الأساليب التي قد يلجأ إليها الجاني، أن يقوم بالاتفاق والتعاقد عبر الانترنت، مع شركة معينه وشراء بعض من منتجاتها، ويتفق على أن تدفع الشيكات عند تسلم البضاعة فيقوم بإرسال سائق شحن يتم استئجاره من أحد الميادين، ويطلب منه أن يجلب له البضاعة من عنوان الشركة، وإعطائه المغلف الذي يحتوى على الشيكات التي بحقيقة الأمر هي غير صحيحة، وتسليمه لإدارة الشركة، ونقل البضاعة إلى مكان يتفق معه عليه ثم عند وصول البضاعة يفرغها لينقلها في عربة شحن أخرى، ويودعها في المكان الذي سوف تباع من خلاله البضاعة كل ذلك دون أن يكون له، أي تواجد، أو مشاهده بين أطراف العملية الاحتيالية، مستغلاً بعض الأفراد، ليقوموا بذلك مقابل أجر، شأنه شأن أي تاجر.

ومن الجدير بالذكر، أن مثل هذه الطريقة الاحتيالية سابقة الذكر باتت من السيناريوهات المكشوفة لكثير من الجهات الأمنية، وإنّه تمت الإشارة إليها في العديد من نشراتها، التي تساعد على أخذ الحيطة والحذر، أثناء التعاملات التجارية والمالية بين الأفراد، لذلك لا يكون بوسع هذه الشركات المستهدفة، سوى اتخاذ الاحتياطات اللازمة للقيام بأي عمل أو نشاط تجاري، باستخدام تكنولوجيا المعلومات[2].

(3) الاحتيال على المصارف : من خلال عمليات الاحتيال بالتحويل المصرفي، داخل البنوك والتلاعب به والاحتيال من خلال بطاقات الدفع الإلكتروني بأنواعها[3]، وسنكتفي بالإشارة فقط إلى هذا النوع من الاحتيال

---

(1) http://www.abuharoon.com/?p=1879

(2) العريفي، جوهرة بنت عبدالعزيز، (2011)، الخداع داخل الانترنت، مركز التميز لأمن المعلومات، متوفر عبر الموقع: www.coeia.edu.sa.

(3) الغثبر والقحطاني، أمن المعلومات، ص35.



الإلكتروني، على المصارف لنخصص الحديث عنه في قسم مستقل فـــي الفصل الثاني من موضوع البحث.

3.1 أركان الاحتيال الإلكتروني ووسائله والنتائج المترتبة عليها:

إن ارتكاب أي جريمة وخروجها إلى حيز الوجود، يتوجب أن تتوافر فيهـــا الأركان والشروط، التي رسمها المشرع، ولعدم وجود نص تشريعي لأركان جرائم الاحتيال الإلكتروني نستخلص هذه الأركان المفترضة، الركن المـــادي ووســـائله، ونتناول ذلك من خلال الـ جزالأول، والشروع في جرائم الاحتيال الإ لكتروني، من خلال الجزء الثاني، القصد الجرمي للجريمة من خلال الجزء الثالث.

1.3.1 الركن المادي لجريمة الاحتيال الإلكتروني و وسائله

وسوف نقوم بدراسة:

أولاً: النشاط الجرمي في جريمة الاحتيال الإلكتروني و وسائله

يُثارُ التساؤل في جرائم الاحتيال الإلكتروني، حـ ول مدى انطباق أفعال هـــذا الجرم مع الأفعال المادية، في جريمة الاحتيال العادية، من حيث تطابق هذا السلوك الذي يقوم به الجاني باستخدام الطرق الاحتيالية، مع أن الأمر لا يختلف كثيراً مـــن حيثُ وجود تلك العناصر والمتمثلة في إيهام المجني عليه، والاستيلاء على مالـــه، بناء على وسائل احتيالية، مع الاختلاف بالأداة المستخدمة، ومن هنا يتضح لنـــا أن الركن المادي لجرائم الاحتيال الإلكتروني، يتكون من ثلاثة عناصر يجب توافرهـــا وهي[1]:

(1) وجود فعل مادي، أي نشاط يقوم به الجاني مستخدما بذلك أي من الوســـائل الاحتيالية.

(2) حدوث نتيجه والمتمثلة بالاستيلاء على مال الغير.

---

(1) الربيعي، حيدر غازي، (2008)، جريمة الاحتيال في مجال التجارة الإلكترونية، مجلة القادسية للقانون والعلوم السياسية، العدد الثالث، ص11.



(3) وجود رابطة سببية بين الفعل والنتيجة المتحققة[1].

أولاً: الأفعال الاحتيالية:

الاحتيال الإلكتروني يقوم في جوهره على الغش والكذب والخداع، فيلجأ الجاني إلى استخدام الطرق الاحتيالية، وتغيير الحقيقة لكي يظفر في مال المجني عليه، دون وجه حق، فيقوم الجاني باستغلال الفضاء الإلكتروني، فالجاني عندما يدعي أنّه مستوردٌ لأجهز ة الحاسب الآلي على سبيل المثال، من خلال شركة يملكها، يقوم بمراسلة عدد من الشركات المعروفة لتزوده ببعض هذه الأجهزة، فإنّ مُجرد كذبه وادعائه لا يشكل جريمة احتيال، بـ ل يتوجب عليه أن يدعم هذه الأكاذيب ببعض المظاهر الخداعة، والتي من شأنها، أن تساهم في إيهام المجني علية، بحيثُ يجعل لهذه الشركة الوهمية موقعاً الكترونياً مثلاً، حيث يتمكن من الدخول والتواصل، من خلاله باسم هذه الشركة، وابتكار عدد من الصور، ونشرها ليبين نشاط و حجم أعماله الوهمية، ويدعم اكاذيبة أيضاً من خلال عدد من الأمور الإجرائية المتعارف عليها في كبرى الشركات، بحيث يلجأ إلى عدد من المشاركين معه، في الكمين الاحتيالي، وإيهام المجني علية بوجود كادر من الموظفين، لبث روح الثقة لدى المجني عليه، ثم يقوم بالتلاعب بالبـ يانات ومخرجات المعلومات، التي من شأنها تسريع وتسهيل عمليه النقل والاستيلاء على المال[2].

ومن هنا يتوجب على الجاني المحتال، لكي يستطيع ممارسة أعماله الاحتيالية بصورة الكترونية، أن يكون قادراً على الإلمام ولو بالحد الأدنى، بتقنية أجهزة الحاسب الآلي، وكيفية استخدامه، وتسخيره للوصول إلى مبتغاه الاحتيالي الجرمي، وأن يمتلك الأداة، التي يجعل منها وسيلته الاحتيالية، مثل امتلاكه أجهزة الحاسب الآلي، وكل ما يتصل بها من الاسطوانات المضغوطة، والأقراص المدمجة، ووصلات تغذية الإنترنت وغيرها من الأدوات الإلكترونية[3]، وقد يلجأ الجاني المحتال إلى الإعلان والتسويق، والنشر لمشروع وهمي على الشبكة العنكبوتية، مثل

---

(1) مصطفى، جرائم الحاسبات الآلية في التشريع المصري، ص99.

(2) قورة، جرائم الحاسب الآلي الاقتصادية، ص429 وما بعدها.

(3) المحمدي، إرهاب الانترنت الخطر القادم، ص62.

امتلاكه شركة لتوزيع وشراء أجهزة وأدوات الحاسب الآلـــي، مـــع ذكـــر بعـــض المواصفات المتعارف عليها في الوسط الإلكتروني، لزرع الثقة في نفس الغير، كما يدخل في سلوك الجاني من خلال ا لركن المادي للجريمة، أنّه قد يقوم بأفعـــال مـــن شأنها المساعدة في توفير المعلومة، التي سوف يستخدمها في جريمته، مثل أن يقوم بالتنسيق مع بعض العاملين بالشركات المستهدفة، أو بأي وسيلة لجمع المعلومة، كأن يدّعي ّأنّه منّ فرق الصيانة لأنظمة الحاسب الآلي، محاولاً الوصًو ل إلى المعلومات، وكيفية الولوج إليها، وكسر أنظمة الحماية، مع إيهام المتعامل معه لتسهيل المهمـــة عليه، والحيلولة دون اكتشاف أمره[1].

أيضاً يتمثل ذلك من خلال استغلال الجاني، لصفة معروفـــة لـــدى إحـــدى الشركات، تحمل الجاني على منحه الثقة، وأنّه قد يكون عامل لدى هـــذه الـــشركة بالفعل، لكن لا تتوفر لديه الصلاحيات، بأن يتعامل مع أنظمة المعلومـــات داخـــل الشركة، أو تبادلها مع باقي الشركات، فمن خلال هذه الصفة، قد يستطيع الولـــوج والتلاعب بالبيانات والمعلومات، ويمارس أساليبه الاحتيالية، وتحويل الأموال باسم غيره، دون أن يكون هناك وجو د لشخصيته الحقيقيـــة، أي إثبـــات فـــي التعامـــل والتلاعب الذي حدث [2]، وأن كل هذه الأساليب والأنشطة، التي يعتمد الجاني فـــي ممارستها بصورة غير مشروعة، تهدف إلى إيهام المجني علية وإيقاعـــه بـــالغلط، مستخدماً الطرق الاحتيالية الخادعة، ومتلاعباً بالأداة التي يرتكب من خلالها جريمته الاحتيالية، وتطورها وشح المعلومات المكتشفة عنها، فيتوجب علينا أن نـــدرك إن

---

(1) زين الدين، بلال، (2008)، جرائم نظم المعالجة الآلية للبيانات، الطبعة الأولى، دار الفكر الجامعي للنشر، الإسكندرية، مصر، ص130 وما بعدها.

(2) Ryan, p. & Harbison, A., (2010) , The Law on computer Fraud in Lreland, development of law and dishonesty, Grant Thorton.p2&3.

نلاحظ أنه ومما سلف يتأكد، لنا أن الأركان المكونة للعديد من جرائم الاحتيال الإلكتروني، من الركن المادي، والركن المعنوي، هي في الواقع تتطابق وأركان جريمة الاحتيال بمفهومها التقليدي، في حين أن الاختلاف ينصب على الوسائل المستخدمة فيما بينهما، وأن ما سيرد من وسائل لجرائم الاحتيال الإلكتروني، ليست على سبيل الحصر؛ لأن مثل هذا النوع كما بينا سابقاً قائماً على الابتكار والتطوير. قورة، جرائم الحاسب الآلي الاقتصادية، ص421.

أجهزة الحاسب الآلي، تعتبر بالغالب المركز الرئيس، الذي من خلاله ما تتم ربط معظم المعلومات والبيانات ومعالجتها، في مراحل الإدخال والإخراج، عن طريق البرامج المختلفة، حسب نوع وغاية هذه البرامج، خصوصاً أن هنالك تنافس، بين كبرى الشركات المتخصصة بإنتاج برامج الحاسب الآلي[1].

ومن الممكن أن نُجمل وسائل الاحتيال الإلكتروني من خلال ما يلي:

(1) التلاعب بالمدخلات: (Input Manipulation)

من الممكن أن نعتبر وبصفة عامة، أن مرحلة التلاعب بالمدخلات، تعد من أكثر حالات الاحتيال الإلكتروني انتشاراً، والتي تنطوي بذاتها على التلاعب بالبيانات والمعلومات، التي يتم إدخالها إلى الأنظمة الإلكترونية، باستخدام أجهزة الحاسب الآلي، وتتم عملية الإدخال "Input"، من خلال تزويد أجهزة الحاسب الآلي والنظام بالبيانات، والمعلومات المراد معالجتها، والتحكم بها آلياً وإدارتها، وتأخذ هذه العمليةِ، في مرحلة الإدخال، عدة وسائل تتمثل فيما يلي[2]:

(أ) تتمثل هذه الصورة والوسيلة، في تغيير البيانات والمعلومات، المراد إدخالها إلى النظام المحوسب، أو المساس بها، أو حذف أي جزء منها، والمسماة بطريقة (Alteration) سواء أكان هذا التغيير والزيادة أثناء عملية الإدخال، أم أثناء مرحلة الإعداد اللازمة للإدخال، وتشمل عملية التغيير والتلاعب بكامل المعلومات، أو جزء فقط منها، وبهذه الحالة، نكون أمام معلومة مغلوطة غير المعلومات الحقيقية، ليسهل الجاني على نفسه، ممارسة إجرامه الاحتيالي، دون أن يُكتشَف أمره والاستيلاء على أموال الغير[3].

(ب) الوسيلة الثانية والتي تسمى (Erasure)، التي تقوم على حذف كافة البيانات أو جزء منها، أثناء مرحلة الإعداد للإدخال، أو أثناء عملية الإدخال، أي عدم

---

(1) المحمدي، إرهاب الانترنت الخطر القادم، ص65 وما بعدها.

(2) المومني، الجرائم المعلوماتية، ص195.

(3) راجع ندوة المعلوماتية القانونية والمنعقدة في طرابلس في الفترة بين 1998/10/13 ولغاية 1998/10/16 والمنشور في مجلة نقابة المحامين الأردنيين العددان العاشر والحادي عشر، 1998، ص3457.

إدخال المعلومات التي كان من المتوجب إدخالها، وتغيير صحة هذه المعلومات والبيانات، وإدخال ما يتناسب وغاية الجاني المحتال من بيانات تـؤدي إلـى احتياله على الآخرين(1).

(ج) الوسيلة الثالثة والمستخدمة بالتلاعب بالبيانات، أثناء مرحلة الإدخال والمسماة (suppression) والمتمثلة في إدخال المعلومات في غير الشأن المخصص لهـا وإخفائها، بحيث تكون غير مشاهدة لمن أراد استخدامها، أي تعطيل الفاعليـة، التي من أجلها تم إدخالها وإعاقة عمل تلك المعلومات، إذاً الجاني إمـا يعـدل المعلومة، أو يغيرها، أو يحذفها، أو يحذف جزء منها من أجل تسهيل عمليتـه الاحتيالية، أو أن يقوم باستخدام هذه الوسائل مجتمعة(2).

(2) التلاعب بالبيانات والمعلومات في مرحلة الإخراج (Out put manipulation)

إن هذا النوع من التلاعب، يعد أقل منه في مرحلة الإدخال، ويأتي تنفيذ مثل هذا النوع من الاحتيال في هذه الحالة بإخفاء المعلومـات والبيانـات فـي لحظـة إخراجها من أجهزة الحاسب الآلي، وفي الغالب تكون من أجل إخفـاء المعلومـة الحقيقية، وعدم استخدامها بالشكل الصحيح، الذي أُدخلَتْ وأُخرجَتْ من أجله، وتـتم هذه الطريقة في مرحلة إخراج المعلومات والبيانات، من خلال تعديل وتغيير هـذه المعلومات التي سبق تخزينها عند مرحلة الإخراج، واسـتعادتها وجعلهـا مخالفـه للحقيقة التي كانت عليها سابقاً سواءٌ بحذّف جزء منها (3)، أو من خلال إضافة جزء من المعلومات إليها، والتي يرغب الجاني بوجودها ومن الأمثلة على ذلك:

قيام أحد مدراء المصارف، أو الشركات الماليـة الاسـتثمارية، بالتلاعـب بالمعلومات والبيانات، عند مرحلة الإخراج، من أجل التستر على جريمتـه، مـن خلال ذلك النظام الإلكتروني، على اعتبار أن مثل هذه الأنظمـة، دائمـاً مـا يـتم

---

(1) قورة، جرائم الحاسب الآلي الاقتصادية، ص438.

(2) المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية، ص331.

(3) Jarret, M. & Bailie, M., (2008) , Prosecuting Computer Crimes, office of legal Education Executive office for United states Attorneys. p12.



مراجعتها وتدقيقها، فيعهد الجاني إلى نفسه، مهمة التلاعب بهـا لكـي لا يُكتـشَف أمره[1].

(3) التلاعب بالبرامج (Programs Manipulation):

إن التلاعب بالبرامج، هو من الحالات الأقل حـدوثاً مـن ضـمن جـرائم الاحتيال الإلكتروني بصورة عامه، وإن كانت من أكثرها خطورة؛ لأنها لا تقـع إلا ممن هم مختصين في مجال البرمجة الإلكترونية في عالم البرمجيـات، بحكـم أن البرمجة تنطوي على نوع من التعقيد، ولا يجيدها من هو غير مختص بذلك، علـى عكس مرحلة التلاعب بالبيانات والمعلومات في مرحلة الإدخال والإخراج، والتي لا يشترط بها سوى الإلمام بتقنية واستخدام أجهزة الحاسب الآلي، والتي باتـت مـن ضروريات العصر، لذلك إن التلاعب بالبرامج يعد من أصعب الحالات حتى فـي اكتشافها[2].

ويتم التلاعب بالبرامج من خلال إحدى هاتين الطريقتين وهما:

(أ) تتمثل هذه الطريقة، من خلال التغيير في البرامج الموجودة داخل المؤسـسة المجني عليها، فمن الطبيعي عند إعداد أي من البرامج، أن يتم مراجعتها قبل بدء العمل من خلالها، والتأكد من وجود أي خطأ في تصميمها، فيستغل الجاني المحتال هذه الفرصة من هذه المرحلة، ويقوم بإدخال التعديلات التـي تـتلائم وحسه الجنائي حتى لا يَكتشَف أمره.

(ب) تحدث هذه الطريقة، في أن الجاني المحتال، يقوم بإعداد برنامج خاص قـام بتجهيزه خفيةً وإدخَّاله إلى ذاكرة الجهاز، في محاولة منه لاستخدامه لتخطـي البرنامج الأصلي[3]، والذي في الغالب ما تتوفر به أنظمـة الحمايـة وعـدم

---

(1) زين الدين، جرائم نظم المعالجة الآلية للبيانات، ص142.

(2) حماد، محمد، (2006)، جرائم الحاسوب، الطبعة الأولى، دار المناهج للنشر، عمان، الأردن، ص154.

(3) العبودي، عباس، (2010)، تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، ص24.

التلاعب، فهو بهذه الحالة يحاول التحايل على الجهاز والنظام أولاً، ثم ينفذ عمليته الاحتيالية والاستيلاء على مال الغير.

(4) التلاعب بالمكونات المادية للحاسب (Hard ware Manipulation)

التلاعب بالبيانات، والمتمثل بجرائم الاحتيال الإلكتروني، غير مقتصر فقد بالتلاعب بالبرامج وأنظمة تشغيل الأجهزة المحوسبة، بل تعدتْ ذلك لتصبح من خلال التلاعب بالمكونات المادية لجهاز الحاسب الآلي، أي العناصر الميكانيكية والتقنية المسيطرة على هذه الأجهزة، والتلاعب بالدوا ئر التي يتكون منها النظام بصورة عامة، ونجد نُدرة في التلاعب من خلال هذه الطريقة، لما تحتاجه من حِرَفية عالية، ومعرفة في التعامل المتعمق مع مكونات وأنظمة الحاسب الآلي، أي أنها تحتاج إلى من هم محترفون في هذا المجال، وللإيضاح نذكر هذه الواقعة، وكيفية التلاعب بالمكونات المادية للحاسب الآلي[1].

وتتلخص هذه الواقعة بقيام إحدى الشركات (The Argent Corporation) والتي تدير أربعة أندية للعب القمار، في لاس فيجاس في الولايات المتحدة الأمريكية، بالاستيلاء على مبلغ يقارب السبعة ملايين دولار، على شكل عملات معدنية، قيمة كل قطعة منها ربع دولار، خلال فترة لم تتجاوز الثمانية عشر شهراً، وتمت هذه العملية الاحتيالية فائقة التعقيد، والتي كانت تعتمد بشكل أساسي على وزن مبرمج بطريقة آلية، فالعملات المعدنية النقدية، كان يتم نقلها من الآلات المخصصة للعب إلى هذا الجهاز، والذي كان أحد الم هندسين الذين ساهموا في تصميم هذا الجهاز، قد تم الاتفاق معه وتجنيده من قبل شركة (The Agent) بحيث قام هذا المهندس، بالتلاعب في الدوائر الإلكترونية للجهاز بحيث يعطي وزن الصناديق بشكل أقل من الحقيقة، والاستيلاء بهذه الحالة على القيمة المتبقية من النقود، والتي لم تحتسب من الوزن الحقيقي[2].

(5) التلاعب بالبيانات التي يتم تحويلها عن بعد.

---

(1) مصطفى، جرائم الحاسبات الآلية في التشريع المصري، ص43 وما بعدها.

(2) الشوابكة، جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، ص179.

وتعد هذه الطريقة أكثر الطرق الاحتيالية تطوراً وابتّكـــاراً والمّـــسماة (Remote System manipulation) أي التلاعب بالبيانات، من خلال النهاية الطرفية أياً كان موقعها، جعل من جرائم الاحتيال الإلكتروني، أكثر إنتشار وسرعة، وصعب من عملية اكتشافها، فيكفي لجهاز الحاسب الآلي، أن يكون متصلاً بوحدة التـــشغيل المركزية، عن طريق شبكة الهاتف العادية (وصلات)، أو شبكة الهواتف اللاســـلكية (تغذية الأبرلكج) يتمكن الجاني المحتال، من الدخول إلـــى المؤســـسة المجـ ـنـــي عليها، أو أي من أجهزة الآخرين ذات الأهمية، من خلال منزله واستخدامه لهـــذه التقنية ووسائل الاتصال المحلية والدولية، وجعل منها فضاءً لجرائمه، في حـــين أن هذه الطريقة بالتلاعب بالبيانات عن بعد، كثيراً ما تستخدم فـــي ارتكـــاب جـــرائم التجسس، وبهذه الحالة يتم تحويل الأ موال، بالتلاعب بالبيانات والأرصدة المالية عن بعد[1].

ومن الملاحظ أن الحالات المرصودة عن الاحتيال الإلكتروني، باســـتخدام طريقة التلاعب بالبيانات عن بعد تقدر بمبالغ كبيرة، وسوف نذكر حالة من أكثـــر حالات الاحتيال الإلكتروني، باستخدام هذه الطريقة تعد من أكثرها شـــ هرة، والتـــي وقعت في نهاية عقد السبعينيات، ومقدار المبلغ المالي الكبير الذي تـــم الاســـتيلاء عليه، وحجم تأثيرها آنذاك لو لم يتم التعامل معها بالشكل الصحيح، ففي شهر مارس من العام 1978 قام أحد الخبراء في مجال أجهزة الحاسب الآلي، والمدعو(Stanly Rifkin mink) أميركي الجنسية، والذي كان يعمل في إحدى البنوك في ولاية لوس انجلوس في الولايات المتحدة الأمريكية، ويـــدعى باســـم (The Security Pacific Bank) بحيث حفظ هذا الشخص، كيفية إجراء عمليات تحويل الأموال الكترونياً داخل البنك، وتمكن من معرفة الشيفرة اللازمة للولوج إلى النظام، وذلك بسبب حرية تنقله بين غرف أجهزة الحاسب الآلي الخاصة بتحويل الأموال بحكم أنّه خبير بالتعامـــل معها[2].

---

(1) إبراهيم، خالد ممدوح، (2011)، حوكمة الانترنت، الطبعة الأولى، دار الفكر الجامعي للنشر، الإسكندرية، مصر، ص141، 142.

(2) الطوالبة، الجرائم الإلكترونية، ص182 وما بعدها.

ومن خلال هاتف ومن خارج البنك، استطاع Rifkin أن يتصل بشبكة المعلومات الخاصة بالبنك مستخدماً شيفرة الدخول، وبحكم معرفته بالإجراءات الأمنية، ونقاط الضعف التي تمكنه من إتمام عمليته، قام بتحويل مبالغ مالية بلغت قرابة العشرة ملايين دولار من البنك إلى حساب خاص به، في ولاية نيويورك، ثم تحويلها إلى إحدى البنوك في سويسرا ، بالرغم من إجراءات المراجعة الدورية، والتدقيق وإجراءات الأمان البنكية، إلا أنّه لم تُكتَشفَ هذه ا لجريمة، إلا بعد مرور ثمانية أيام على ارتكابها، وفي العام 1979، تم تقديم المتهم إلى المحاكمة بعدة تهم، تُعد من صميم جرائم الاحتيال الإلكتروني، من خلال التلاعب بالأنظمة البنكية لتحويل الأموال، حيث حكم علية بالسجن لمدة ثماني سنوات، ومقارنةً بالعصر الحالي، نجد أن مبلغ عشرة ملايين دولار، وفقدانه بعملية احتيال الكتروني، كفيلة بإغلاق البنك والتسبب بأزمة اقتصادية على الصعيد المحلي، وعلى حقوق الأفراد والدخول بدائرة مفرغة، يصعب الخروج منها، فكيف هو الحال في نهاية عقد السبعينيات، وإنْ كانت المصارف والبنوك الأمريكية، تُعد من الأقوى على الصعيد الدولي(1).

(6) استعمال شيفرة غير صحيحة للدخول إلى نظام مدفوع الأجر:

والمقصود باستعمال هذه الشيفرة : هو الدخول إلى هذا النظام مدفوع الأجر، مستخدمين شيفرة مملوكة إلى شخص آخر، أو من الممكن أن تكون هذه الشيفرة، مملوكة للنظام نفسه، بحيث يتمكن الجاني المحتال، من الحصول على أرقام هذه

---

(1) إبراهيم، حوكمة الانترنت، 143 وما بعدها. تجدر الإشارة إلى أن كل من وحدات الإدخال، والإخراج، هي من العناصر المكونة لأجهزة الحاسب الآلي ويمكن تعريفها:

(أ) وحدات الإدخال: وهي مجموعة من الأدوات التي تعمل على إدخال البيانات والمعلومات، إلى أجهزة الحاسب الآلي، وتشمل لوحة المفاتيح، الفأرة، والميكرفون، والماسحة الضوئية.

(ب) وحدات الإخراج: وهي التي يُعهد إليها مهمة إخراج المعلومات والبيانات، وإظهار النتائج بعد معالجتها، من خلال هذه الأجهزة، مثل الشاشة، والطابعة، والسماعات وغيرها....أنظر ذلك نسرين عبدالحميد نبيه، مرجع سابق، ص8 .

الشفيرة، قبل أن تباع فالمقصود بعدم صحة الشيفرة ليس بالضرورة أنها مقلـــدة، أو مسروقة، إنما يتم استخدامها، من قبل شخص لا يحق له استخدامها(1).

ومن أهم الأمثلة المشهورة على هذه الوسيلة، هي الحكم في قضية (Gold) وشريكه (Schifrin) في المملكة المتحدة، وتتلخص أحداث القضية في حصول كـل من المدعو (Gold) وشريكه على الشيفرة الخاصة، التي أصدرتها هيئة الاتصالات البريطانية لأحد المهندسين العاملين لديها، لكي يتمكن من خلال هذه الشيفرة، مـن استخدام نظام المعلومات الإلكتروني الخاص به، (Presler System) وهـذا النظـام عبارة عن قاعدة من البيانات، تسمح للمشتركين الدخول إلى نظام المعلومات، مقابل رسم يدفع عند الدخول، بالإضافة إلى مقابل نقدي يدفعه المشترك المستخدم، بحسب حجم المعلومات، والبيانات التي يطلبها، ومن خلال بطاقة المهندس تمكـن (Gold) وشريكه من دخول النظام بدون رسم اشتراك، والحصول على المعلومات والبيانات اللازمة، دون أن يتحملا أي نفقات، مكررين هذه العملية، ومع مرور الوقت، بدأت هيئة الاتصالات البريطانية، بمراقبة المدعو Gold ودخوله دائرة الشك لديهم، ليـتم بعد ذلك الكشف عن نشاطه وشريكه، والإمساك بهم وتقديمهم إلى العدالة، فلم يوجد نص قانوني صريح يجرم أفعالهم، سوى قانون السرقة وقانون التزوير، مما كـان لهذه القضية الدور البارز، الذي دفع المشرع الإنجليزي، إلى إصدار قانون إسـاءة استخدام الحاسب الآلي في العام 1990(2).

ثانياً: النتيجة الإجرامية في جرائم الاحتيال الإلكتروني

يجب أن تؤدي الوسائل الاحتيالية التي يستخدمها الفاعل، والتي نص القانون عليها إلى أيهام المجني عليه، وإيقاعه بالغلط، الذي يحمّله إلى تسليم المال للجـاني

---

(1) السرحان، سرحان سليمان؛ والمشهداني، محمود، (2001)، أمن الحاسوب والمعلومات، دار وائل للنشر، عمان، الأردن، ص49.

(2) قورة، جرائم الحاسب الآلي الاقتصادية، ص456 وما بعدها. تجدر الإشارة إلى أنه شاع بالولايات المتحدة الأمريكية، استخدام مصطلح soft ware للدلالة على البرامج، في حين استخدم مصطلح Hard ware لدلالة إلى جهاز الحاسب الآلي نفسه، أو كما يسميه البعض الحاسب الإلكتروني، حماد، جرائم الحاسوب، ص43.

مرتكب الفعل لكي تكتمل الجريمة، فالجاني لايكفي منه فقط، أن يقوم بالأفعال مستخدماً وسائل احتيالية، بدون تحقق نتيجة جرميه وهي تسليم المال، وهذا التسليم الذي يتم من خلال المجني عليه، يجب أن يكون سببه الإيهام والغلط، الذي وقع به، وليس أي سبب آخر لكي لا تنقطع معه علاقة السببية[(1)].

فالأمر لا يختلف بشكل عام، في الاحتيال الإلكتروني، عنه في جريمة الاحتيال التقليدية، فالجاني المستخدم للأساليب الاحتيالية بالصورة الإلكترونية، يجب أن يؤدي نشاطه إلى نتيجة تكتمل معها الجريمة، وتتحقق النتيجة بتسليم المال من المجني عليه إلى الجاني، ويكون هذا التسليم راجع سببه في المقام الأول والأخير، إلى فعل الإيهام الصا در من الجاني، لعدم قطع علاقة السببية لنتيجة الجرمية، وهي تسليم المال للجاني مرتكب الفعل [(2)]، ومن أجل فهم المقصود بتسليم المال، وهل هو نفسه المقصود بجريمة الاحتيال التقليدية، نقف عند هذا المفهوم بشيء من الإيضاح.

بما أن التسليم هو ثمرة الإيهام والغلط الذي وق ع به المجني عليه، فأنه يؤدي إلى نقل ملكية وحيازة هذا المال، وفي الغالب ما نلاحظ أن التسليم في جرائم

---

(1) البحر، الجرائم الواقعة على الأموال في قانون العقوبات الإماراتي، ص222.

(2) زين الدين، جرائم نظم المعالجة الآلية للبيانات، ص152. مع الإشارة إلى أن تقنية المعلومات تعني: أية وسيلة، أو مجموعة وسائل مترابطة، أو غير مترابطة، تستعمل لتخزين المعلومات واسترجاعه، أو معالجتها وتطويرها وفقاً للأوامر، والتعليمات المخزونة، ويشمل ذلك جميع المدخلات والمخرجات المترابطة بها، لاسلكياً في نظام، أو شبكة.

(أ) البيانات: هي كل ما يمكن تخزينه ومعالجته، وتوليده بواسطة تقنية أنظمة المعلومات، كالأرقام، والحروف، والرموز، وما إلى ذلك. أنظر نص المادة الأولى من قانون المعاملات الإلكترونية المؤقت رقم (85) لسنة 2001. في حين يرجع الفضل إلى الأستاذ الفرنسي Drefus في اقتراح مصطلح المعلوماتية، عندما استخدمه في العام 1962، لتمييز المعالجة الآلية للمعلومات، في حين تبنت الأكاديمية الفرنسية مصطلح المعلوماتية في العام 1966، وعرفته على أنّه: علم المعالجة المنطقية للمعلومات، والتي يعتبر بمثابة دعامة للمعارف الإنسانية، والاتصالات في المجالات الفنية، والاقتصادية، والاجتماعية، وذلك باستخدام معلومات آلية. العريان، الجرائم المعلوماتية، ص18.

الاحتيال التقليدية يتم بصورة مباشرة من المجني عليه إلى الجاني، فهل من الممكن أن يتم التسليم بصورة مادية، أو غير مادية بالنسبة إلى جرائم الاحتيال الإلكتروني؟

من الممكن أن يتم التسليم بصورة مادية من قبل المجني عليه، ولكن بـــدون المناولة المباشرة للجاني، مثل استخدام البطاقـــات الائتمانيـــة مـــن قبـــل الجـــاني، والاستيلاء على مال الغير من خلال هذه البطاقة بصورة مادية، أما التسليم بصورة غير مادية نجد إن مثل هذا التسليم أيضاً ، ينطبق عليه مفهوم تسليم المال في جريمة الاحتيال الإلكتروني، فإن الجاني عندما يقوم بالاستيلاء على مال الغير، من جـــراء تعامله مع المجني عليه من خلال التلاعب تكنولوجيا المعلومات وأنظمتها، فإن إرادة المجني عليه تتجه إلى وضع المال تحت يد الجاني، وهذا يعد بمثابة تسليم للمال من قبل المجني عليه إلى الجاني، وإذ لم يكن بصورة مباشرة أي (بالمناولة)[1].

ويتوجب أن يكون محل هذه الجريمة، مالاً له قيمة في نظر القانون، أما من يستولي على منفعة من الغير، فلا يمكن أن نصنفها احتيالاً، وبالرغم من اصـــطدام فكرة المال المادي الملموس مع جرائم الاحتيال الإلكتروني، في بعض الحالات مثل استخدام شيفرة مدفوعة الأجر، للدخول إلى نظام، وأخذ المعلومات بدون دفع ثمنها، والتي لا تنطبق وفكرة المال المادي الملموس، إلا أنها تصح لتعتبر مالاً في نطـــاق جرائم الاحتيال الإلكتروني [2]، فإنْ كان بمقدور الجاني المحتال، الحصول على المال بصورة مادية ملموسة، تتطابق وفكرة المال في جرائم الاحتيـــال التقليـــدي، مثـــل الاستيلاء على المال من خلال بطاقات الصراف الآلي، بعد الحصول علـــى الـــرقم السري للبطاقة، إلا إن هنالك من حالات الاحتيال الإلكتروني، والتي تمثل ما نـــسبة 70%من هذه ا لجرائم تتم بصورة كتابية، مثل التلاعب بالبرامج، وفي هذا الـــسياق نجد أن هنالك تباين بين التشريعات، في اعتبار مثل هذه الأموال الكتابيـــة، محـــلاً لجرائم الاحتيال الإلكتروني فبعض التشريعات ومنها التشريع الألماني، والتـــشريع

---

(1) الفيل، الإجرام الإلكتروني، ص32، 33.

(2) الملط، أحمد خليفة، (2001)، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، مصر، ص338.



الياباني، ذهبا إلى عدم أمكانية اعتبار هذه ا لأموال الكتابية، محلاً لجرائم الاحتيال الإلكتروني[1].

في حين ذهبت غالبية التشريعات، إلى عكس ذلك، وأخذت بصحة اعتبار مثل هذه الأموال الكتابية، محلاً لجريمة الاحتيال الإلكتروني، والسرقة أيضاً، ومنها التشريع الكندي، الهولندي، السويسري، الانجليزي، والتشريع الأ ردني، والتشريع المصري بحيث أن التسليم يتحقق بمجرد وضع هذا الشيء ذو القيمة القانونية، تحت أمر وتصرف الجاني المحتال[2].

ولكن يثار التساؤل حول إمكانية أن يكون محل الاحتيال الإلكتروني عقاراً.

بالرجوع إلى نص المادة (336) من قانون العقوبات المصري، والذي حدد أن جرائم النصب لا تقع إلا على مال منقول، ولا تقع على عقار، وبذلك لا يمكن أن يكون محل مثل هذه الجرائم عقاراً، وعلى خلاف ذلك المشرع الأردني، الذي أشار إلى أمكانية أن يكون محل جرائم الاحتيال، مالاً منقولاً أو عقار من خلال نص المادة (417) فلن نصطدم مع أمكانية شمو ل العقار، لجرائم الاحتيال الإلكتروني، إما المشرع الفرنسي، والذي كان قد أشار في نص المادة (405) من قانون العقوبات الملغى، إلى جرائم الاحتيال فإنّه لم يكن هنالك ما يكفي من الوضوح، حول شمول العقار لهذه الجرائم، واختلفت الاجتهادات حول ذلك، إلى أن جاء القانون الجديد ليفصل بالأمر، ويجعل من العقار محل لجريمة الاحتيال، من خلال نص المادة (313) من قانون العقوبات، فعند النظر لجرائم الاحتيال الإلكتروني، من الناحية النظرية فإنّه لا خلاف على العقار ، في اعتباره محل لهذه الجرائم شأنه شأن المال المنقول[3].

ومن جهة نظر البا حث، أن التلاعب بالبيانات والبرامج وتحويل وانتقال هذه الأموال، نجد أن كل ما يندرج تحت مسمى مال ذو قيمة، بات يتحكم به من خلال أنظمة وأجهزة الحاسب الآلي، والبرامج المحفوظة المعدة لهذه الغاية، وأنّه لا بديل

---

(1) الشوابكة، جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، ص191.

(2) قورة، جرائم الحاسب الآلي الاقتصادية، ص468.

(3) العريان، الجرائم المعلوماتية، ص127

عن استخدام تكنولوجيا المعلومات في مختلف المجالات، لما تمتاز به من سرعة وازدياد واضح في عدد الأفراد واحتياجاتهم، بحيث أنّه من الممكن أن تتم عملية الاحتيال، من خلال تحويل نقل ملكية عقار مثلاً، من خلال التواطيء بالاتفاق مع أحد العاملين بدائرة التسجيل، لقاء إعطاء هذا الموظف مبلغ من المال، لكي يسهل مهمة هذا الجاني المحتال، وإدخاله كشريك في هذا الجرم الاحتيالي، واستغلاله لمنصبه الوظيفي من أجل إيهام المجني عليه، بعد التلاعب بالمدخلات والبيانات الخاصة بذلك العقار الكترونياً ً(1)، خصوصاً إذا كان المالك من الفئة غير المتعلمة، أو من كبار السن وغير مواكب ومدرك للتعامل بثورة تكنولوجيا المعلومات، والمخاطر المتمخضة عنها، وفي هذه الحالة من غير المتصور، عدم اعتبار ذلك من ضمن جرائم الاحتيال الإلكتروني، سيما وأن مفهوم الحماية القانونية لحقوق الأفراد، تشمل كل ما له قيمة مادية، ومثل هذا النوع من القيم المادية للأفراد (العقار) قد تكفلت به معظم التشريعات، بتوفير الحماية الجزائية لها، خصوصاً أن هذا النوع من الجرائم قائمٌ على التطور والابتكار، وليس له من الضوابط المستقرة، التي يمكن من خلالها تحديد ما قد تشمله هذه الجرائم الاحتيالية في المستقبل (2) وهو ما يتفق الباحث معه في التشريع الأردني لشموله العقار بغية توفير حماية أكبر للحقوق.

---

(1) تجدر الإشارة إلى أنه لا يوجد حالات واقعية لعمليات احتيال الكتروني، وقعت على عقار في الأردن والسبب يرجع بذلك، إلى تعقيد إجراءات عملية نقل ملكية مثل هذه الأموال، والتي تتطلب في كثير من الأحيان تواجد صاحب العقار، ووجود شهود وإن حتى آلية التعامل مع هذه المعاملات عن طريق برامج الحاسب الآلي، وتكنولوجيا المعلومات، ليس بالصورة المطلقة الكاملة، كما هو الحال بالنسبة لباقي الأموال، بل إن هنالك إجراءات كتابية كثيرة لا تتم فيها عملية نقل العقار، إلا من خلال موظفي دائرة الأراضي، وأكثر من جهة ودائرة رسمية تتبع لذلك.

(2) أن المشرع الأردني، ومن خلال جواز أمكانية اعتبار العقار محل لجرائم الاحتيال التقليدية، فإنه سد باب الاجتهاد والخلاف، وأي تعارض في الأحكام، مما ساعد في توفير الحماية الجزائية للحقوق والأموال، بصورة أكثر فاعلية، على خلاف ما قد نراه في بعض التشريعات، كالتشريع الفرنسي الملغى والتشريع المصري، والجدل والاجتهاد في اعتبار العقار ومساواته بالمال المنقول، كمحل لجرائم الاحتيال الإلكتروني من عدمه.

2.3.1 الشروع في جرائم الاحتيال الإلكتروني:

يعاقب المشرع الأردني على الشروع في جريمة الاحتيال التقليديـــة، حيــث نصت المادة (417) الفقرة الثالثة، بعد أن بينت وسائل الاحتيال، وعقاب الجريمـــة التامة على الشروع أنه : "يطبق العقاب نفسه على الشروع في ارتكـــاب أي مـــن الجنح المنصوص عليها في هذه المادة " حيث ساوى المشرع، بين عقوبة الجريمـــة التامة والشروع فيها، والشروع كما أورده قانون العقوبات الأردني، شروع تام من خلال نص المادة (70) وشروع ناقص من خلال نص المادة (68) ومن خلاله يمكن تعريفه على أنه:

الشروع التام: وفيه يحقق الجاني النشاط الإجرامي كاملاً، وبالرغم من ذلك فإنّ النتيجة الإجرامية، لا تتحقق لأسباب لا دخل لإرادته فيها، وهو ما يطلق عليـــه بالجريمة الخائبه، أما الشروع الناقص : وهو الذي لا يكتمل به النشاط الإجرامـــي، لسبب أيضاً خارج عن إرادة الفاعل ويطلق عليه الجريمة الموقوفة(1).

أما فيما يتعلق بالشروع في جريمة الاحتيال الإلكترونـــي، نجـــد المـــشرع الأردني من خلال قانون جرائم أنظمة المعلومات المؤقت رقم (30) لسنة 2010، قد جرم عدداً من الأفعال التي تندرج تحت صور الاحتيال الإلكتروني، وعاقب علـ يهـــا بعقوبات جنحوية، ولم يرد في هذا القانون نصوص خاصه بالعقاب على الشروع في هذه الجنح، حيث أن العقاب على الشروع في الجنح في التـــشريع الأردنـــي رهـــن وجود نص يعاقب على ذلك وفقاً لنصّ المادة (71) من قانون العقوبـــات الأردنـــي، على خلاف العديد من التشريعات العربية والأجنـ بية، التي عاقبت على الشروع فـــي هذه الجرائم.

ويرى الباحث أنّه من الممكن تصور الشروع بجرائم الاحتيال الإلكترونـــي، بنوعيه التام والناقص ونستدل على ذلك بالأمثلة الآتية:

الشروع التام: كما لو قام الفاعل بإدخال البطاقة الممغنطة الخاصـــة بجهـــاز الصرف الآلي، وقام بإدخـال الرقم السري الخاص بالبطاقة، من أجل الاستيلاء على

---

(1) المجالي، نظام توفيق، (2005)، شرح قانون العقوبات القسم العام، الطبعة الأولى، دار الثقافة للنشر، عمان، الأردن، ص242.

مال الغير، وقبل نجاح العملية وتسلمه المال، لحق بالجهاز عطل تقني مفاجئ، ففي هذه الحالة نكون أمام شروع تام لأحد جرائم الاحتيال الإلكتروني، كون الجاني استنفذ نشاطه الإجرامي، ولسبب خارج عن إرادته لم تتحقق النتيجة الإجرامية.

الشروع الناقص: كما لو قام الفاعل، بالتلاعب بالبيانات الخاصة لأحد العملاء، بأحد المصارف، من أجل تحويل أمواله، ثم انقطع التيار الكهربائي، ففي هذه الحالة نكون أمام شروع ناقص لأحد جرائم الاحتيال الإلكتروني كون الجاني لم يستكمل الأفعال اللازمة لتنفيذ الجريمة، ونستدل على ذلك من خلال التشريعات، التي عاقبت على جرائم الاحتيال الإلكتروني، وعلى الشروع في هذه الجرائم، ومن هذه التشريعات قانون العقوبات القطري رقم (11) لسنة 2004، من خلال نصوص المواد (370 ولغاية 387) حيث جاء في نص المادة (387) من القانون ذاته العقاب على الشروع أنه : " يعاقب على الشروع في الجنح، المنصوص عليها في هذا الفصل، بما لا يجاوز نصف الحد الأقصى للعقوبة المقررة للجريمة التامة"[1].

كما جرم نظام مكافحة الجرائم المعلوماتية السعودي، رقم (79) لسنة 2007 الشروع في الاحتيال الإلكتروني، حيث اشتمل النظام، على (15) مادة للحد من الجرائم المعلوماتية، فجاء في نص المادة (4)الفقرة الأولى أنه : " يعاقب بالسجن مدة لا تزيد عن ثلاثة سنوات، وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1. الاستيلاء لنفسه، أو لغيره على مال منقول، أو على سند، أو توقيع هذا السند وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.

في حين جاء العقاب على الشروع من خلال نص المادة (10)على أنّـه : يعاقب" كل من شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام، بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة"[2].

---

(1) قانون العقوبات القطري رقم (11)لسنة (2004) متوفر عبر الرابط:
www.gcc_legal.org/mojportalpublic/BrowseLawOption.aspx?country=3&LawID=2597

(2) نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية رقم (79) لسنة 2007 متوفر عبر الرابط: http://www.ala7ebah.com/upload/showthread.php?69359

وعند الحديث عن الشروع في جرائم الاحتيال الإلكتروني، فإنه ينبغي التمييز بينه وبين الأعمال التحضيرية، وأعمالاً لنص المادة (69) من قانون العقوبات الأردني فإن: " مجرد العزم على ارتكاب جريمة، لا يعتبر شروعاً فيها"

فالنشاط الإجرامي لإرتكاب الجريمة، يمر في عدد من المراحل، فتبدأ بالتفكير في الجريمة والتصميم عليها، وهي مرحلة نفسية تكون الجريمة فيها مجرد فكرة، ولا عقاب على هذه المرحلة حتى لو ثبت التفكير في الجريمة، على نحو قاطع[1]، ثم تأتي بعد ذلك مرحلة الأعمال التحضيرية، التي تشمل كل فعل يهدف من خلاله الجاني إلى خلق البيئة المناسبة لتنفيذ الجريمة، ولا عقاب على هذه الأفعال، فالعمل التحضيري مجرد من الأهمية القانونية، لعدم انطوائه على خطر يُهدد به الحق، بالإضافة إلى أنه لا يدّل دلالة قاطعة، على اتجاه الجاني إلى ارتكاب الجريمة، لوجود احتمال عدوله عن البدء بتنفيذ الجريمة التي سبق وأعد لها[2].

وفيما يتعلق بالاحتيال الإلكتروني، فإنه يعد عمل تحضيرياً، كل نشاط يقوم به الفاعل قبل استعماله الوسائل الاحتيالية، بمعني أي نشاط يأتيه الفاعل قبل البدء في تنفيذ الوسائل الا حتيالية، مثل إعداد برامج خاصة به، لكي يدّخلها بجهاز الحاسب الآلي مكان البرام ج الأصلية، فالأعمال التحضيرية تقف عند اللحظة التي يبدأ فيها الفاعل اتصاله بجهاز الحاسب الآلي، من أجل تنفيذ وسيلة الاحتيال، وهو يتفق مع جريمة الاحتيال التقليدية، حيث يعتبر كل نشاط يأتيه الجاني قبل اتصاله بالمجني عليه عملاً تحضيرياً، إذ أن الحد الفاصل بين العمل التحضيري والشروع، هو السعي من أجل الاتصال بالمجني عليه وخداعه، وكل ما يسبق ذلك يعد عملاً تحضيرياً، فمجرد تهيئة جهاز الحاسب الآلي للاتصال، فإنه يُعد من قبيل الأعمال التحضيرية، أما إذا اقترن ذلك باستخدام إحدى الوسائل الاحتيالية، فإنّه يعتبر بدءاً في التنفيذ وشروعاً بّالجريمة [3]، وعليه إذا توقف نشاط الفاعل عند حد العمل التحضيري، فإنّه لا عقاب عليه إذ لا يعد شروعاً في الجريمة، ولكن القانون قد

---

(1) الجيوشي، جرائم الاحتيال الأساليب والوقاية والمكافحة، ص39.

(2) حافظ، جرائم النصب والاحتيال والجرائم الملحقة بها ص52.

(3) قورة، جرائم الحاسب الآلي الاقتصادية، ص481.

يعتبر هذا النشاط جريمة أخرى بحد ذاتها، و مختلفة عن محل التحضير، حيث أن هذا العمل التحضيري ينطوي على خطر يهدد الحقوق، ويشكل خطورة على المجتمع، تقتضي معه العدالة أن تجعل منه جريمة مستقلة، عن الجريمة محل التحضير، متى توافرت شروط وأركان هذه الجريمة[1].

ويُثار ُالتساؤل عن مدى إمكانية تحقق هذا التصور، على الأعمال التحضيرية في جرائم الاحتيال الإلكتروني، خصوصاً أن هنالك من الجرائم ما تقترب كثيراً من العمل التحضيري، لجرائم الاحتيال الإلكتروني، مثل جريمة الدخول غير المصرح به؟

إن التشريعات تباينت، في كيفية تجريم الدخول غير المصرح به، فمنها ما يستلزم توافر القصد الجرمي الخاص للفاعل، بالتأثير على نظام الحاسب الآلي، ومن التشريعات من جعل التجريم بشكل مطلق، وتعاقب بمجرد الدخول دون الحاجة لوجود القصد الجرمي الخاص، أو أي قيود تتعلق بالركن المادي مثل القانون الأردني، حيث جَرمتْ المادة 3/أ الدخول غير المصرح به لأنظمة المعلومات المجرد[2]، والتشريع الفرنسي حيث نصت المادة (323) الفقرة (أ) من قانون العقوبات على أنّه : "يعاقب على الدخول، أو الاستمرار بالبقاء في نظام المعلومات المبرمجة، أو جزء منه - بقصد الغش بالحبس مدة لا تزيد على سنة والغرامة التي لا تزيد عن (100) ألف فرنك"، فهي إذاً جريمة لا تستلزم حدوث نتيجة معينه لأنها تعد جريمة خطر وليس جريمة ضرر، والمقصود بهذه الجريمة : هو دخول الفاعل إلى نظام الحاسب الآلي، دون أن يكون مسموحاً له وهو عالماً بذلك سواء كان يعمل

---

(1) جعفر، قانون العقوبات القسم الخاص، ص153.

(2) تنص هذه المادة على أن: "كل من دخل قصداً، إلى موقع الكتروني، أو نظام معلومات بأي وسيلة دون تصريح، أو بما يخالف، أو يجاوز التصريح، يعاقب بالحبس مدة لا تقل عن أسبوع، ولا تزيد على ثلاثة أشهر، أو بغرامة لا تقل عن (100) دينار ولا تزيد على (200) دينار، أو بكلتا هاتين العقوبتين".

لدى الجهة مالكة جهاز الحاسب الآلي، أو لا يعمل لديها [1]، وهذا ما يمكن تحققه في جرائم الاحتيال الإلكتروني، في حالة وقوف النشاط الإجرامي للفاعل عند حد الاتصال غير المشروع بالحاسب الآلي، فإذا كان النظام على سبيل المثال غير مسموح الدخول إليه، وكان قصد الفاعل من الدخول التحضير للتلاعب في أحد البيانات، كوسيلة من وسائل الاحتيال الإلكتروني، إلا أن نشاطه وقف عند حد هذا الدخول، وهو ما يعد في الأصل عملاً تحضيرياً لجريمة الاحتيال، فإن هذا النشاط يشكل جريمة مستقلة عن الجريمة التي يستهدف الفاعل التحضير لها ألا وهي جريمة الدخول غير المصرح به إلى نظام الحاسب الآلي، متى توافرت أركان هذه الجريمة[2].

وبناءً عليه، فإن الضرورة تقتضي تجريم الشروع في جرائم الاحتيال الإلكتروني، في حالة تجاوز مرحلة الأعمال التحضيرية وفرض العقاب الرادع لذلك، هذا ما دفع بالدول العربية ومن خلال جامعة الدول العربية، إلى تبني مشروع قانون خاص بتقنية المعلومات قدمته دولة الإمارات العربية المتحدة، وتم اعتماده من قبل الدول الأعضاء بالجامعة سنة 2004وحمل اسم " قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها " حيث جاء القانون في (27) مادة، وبعدما تناولت نص المادة الأولى بعض التعريفات الخاصة بتقنية المعلومات حيث جاء في نص المادة (10) من ذات القانون أنه : " كل من توصل عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي وما في حكمها إلى الاستيلاء لنفسه، أو لغيره على مال منقول، أو على سند، أو توقيع هذا السند وذلك بالاستعانة بطريقة احتيالية، أو باتخاذ اسم كاذب، أو انتحال صفةٍ غير صحيحةٍ متى كان ذلك من شأنه خداع المجني عليه، يعاقب بالحبس (حسب كل دول) والغرامة.. أو بإحدى هاتين العقوبتين " فيما بينت المادة (24) التجريم الخاص بالشروع لهذه الجرائم على أنه: يعاقب بالشروع في الجرائم المنصوص عليها في

---

(1) محمد، شيماء عبدالغني، (2007)، الحماية الجنائية للتعاملات الإلكترونية، الطبعة الأولى، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، ص96 وما بعدها.

(2) قورة، جرائم الحاسب الآلي الاقتصادية، ص482.

المواد من (3_15) بنصف العقوبة المقررة لها، ويعاقب بالشروع في الجرائم المنصوص عليها في المواد من (16_22) بذات العقوبة المقررة لها"[1].

أما فيما يتعلق بقانون جرائم تقنية المعلومات الإماراتي، رقم (2) لسنة 2006 والذي احتوى على (29)مادة بخصوص جرائم تق نية المعلومات، ومن ضمنها جرائم الاحتيال الإلكتروني، إلا أنّه لم يتناول نصوص تجرم الشروع الخاص بتلك الجرائم والعقاب عليها، وهو الحال ذاته للقانون العربي النموذجي الموحد الخاص لمكافحة سوء استخدام تكنولوجيا المعلومات والاتصال، والذي اشتمل في نصوصه على (27) مادة تناولت عدداً من الجرائم المعلوماتية، وجرائم الاحتيال الإلكتروني، إلا أنّه لم ينظم الحالة التي يتم فيها الشروع بهذه الجرائم.

ومن التشريعات التي نظمت نصوصاً خاصة بجرائم الاحتيال الإلكتروني، وعاقبت على الشروع بهذه الجرائم على الصعيد الأجنبي، قانون تكنولوج يا المعلومات الهندي (المعدل) لسنة 2008، حيث جاء في نص المادة (74) على أنّه: " كل من يقوم عن إدراك بإنشاء شهادة توقيع الإلكتروني، أو نشرها، أو إتاحتها وذلك لأي غرض احتيالي، أو غير قانوني، يعاقب بالسجن مدة يمكن أن تصل إلى سنتين، أو بالغرامة التي يمكن أن تصل إلى مائة ألف روبية، أو بكلتا العقوبتين"

أما فيما يتعلق بالشروع في الجرائم، التي نص القانون عليها فقد بينتها نص المادة (84) الفقرة (ج) على أنّه: " كل من يحاول ارتكاب جرم من الجرائم، التي يعاقب عليها هذا القانون، أو يسبب ارتكاب مثل هذا الجرم، ويقوم بأي عمل ضمن هذه المحاولة من أجل ارتكاب الجريمة، وليس هناك حكم صريح ينص على معاقبته على مثل هذه المحاولة (الشروع)، فيعاقب بالسجن لأي من الفئات المنصوص عليها لذلك الجرم، مدة يمكن أن تصل إلى نصف مدة السجن القصوى المنصوص عليها

---

(1) قانون الأمارات العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها متوفر عبر الرابط :
http://arabic.mjustice.dz/liguearabe/loi_emir_ar_crim_tech_info.pdf



بخصوص ذلك الجرم، أو بالغرامة المنصوص عليها لمثل هـذا الجـرم، أو بكلتـا العقوبتين"[(1)].

3.3.1 الركن المعنوي لجريمة الاحتيال الإلكتروني

القصد الجرمي في جريمة الاحتيال الإلكتروني، شأنه شأن القصد الجرمـي في جريمة الاحتيال بمفهومها التقليدي، فهي من الجرائم العمدية، والتي يتطلب فيها القصد الجنائي فإذا لـم يتوفر هذا القصد الجرمي، فلا تقوم المسؤولية الجنائية حينها، ويتمثل القصد العام في جريمة الاحتيال الإلكتروني، بأن يعلم الشخص مرتكب الفعل أنّه عند قيامه بهذا السلوك المتمثل بإدخال البيانات والمعلومات، إلى أنظمة جهـاز الحاسب الآلي، وأن من المؤكد استجابة هذا النظام المحوسب، له بناءً علـى هـذه الأوامر، وأن يعلم إن ما يقوم به من إدخال أو إخراج لهذه البيانات والمعلومات، يعد من قبيل التلاعب بها، عندما يقصد إدخال معلومات غيـر المعلومـات المطلـوب إدخالها، أو من خلال تعديلها، أو حذف هذه المعلومات كلها، أو جزء منها، أما من لم يتوفر لديه العلم ولم تتجه أرادته للقيام بهذا التلاعب فأن المسؤولية لا تقوم بحقـه كمن يحاول استخدام بطاقته الإئتمانية التي يملكهـا مـن خـلال إحـدى الأنظمـة المحوسبة، ويحاول الاستفادة منها بشتى الوسائل، وهو لا يعلم أنها أصـبحت غيـر صالحة للاستخدام[(2)].

وأنّهّ لا يـ تطلب من الفاعل، أن يكون على دراية وعلم، بأن هذه الوسائل التي يستخدمها أنها من الوسائل التي أشار إليها القانون وجرمها، ما دام أن إرادته اتجهت إلى القيام بهذا العمل، وأنّه يعلم أن القيام به بحد ذاته مجرّم بغـض النظـر، عـن الوسيلة المستخدمة خصوصاً إن مثل هذه الوسائل دوماً، ما تكون قائمة على الابتكار والتطور وليس على سبيل الحصر، بل يكفي أن تكون هذه الوسـيلة المـستخدمة،

---

(1) قانون تكنولوجيا المعلومات الهندي (المعدل) لسنة 2008 متوفر عبر الرابط:
http://www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf

(2) قورة، جرائم الحاسب الآلي الاقتصادية، ص489.

تنطوي على التلاعب غير المشروع بالبيانات والمعلومات [(1)]، ويتوجب على الفاعل أن يكون عالماً، بأن هذا المال الذي يرغب بالاستيلاء عليه، هو ليس مملوك له، بل من ملك الغير سواء أكان هذا الجاني يعلم شخصية الغير المجني عليه أم لا [(2)]، وكثيراً ما نجد ذلك في العملية الاحتيالية، التي تنفذ في تحويل الأموال عن بعد والتي نلاحظ، أن غالبية هذه الحالات لا يعلم الجاني شخصية المجني عليه، لان الغاية والهدف الأساس للجاني يتمثل بالاستيلاء على مال الغير، بغض النظر عن شخص هذا المجني علية، وأنّه استخدم معلوماته وشيفرته الخاصة المتعلقة بحساباته المصرفية من دون أن تتولد لدية أي حاجة إلى التعرف على شخص هذا المجني عليه، وهذا ما يسعى إليه الجاني دوماً وهو التواري عن الأنظار [(3)].

وبخصوص القصد الجرمي الخاص، نجد أن هنالك جانب من الفقه لا يشترط أي قصد خاص لجريمة الاحتيال الإلكتروني، على اعتبار أن الاستيلاء على المال، هو النتيجة الحتمية لهذا الفعل غير المشروع، فلن تخرج نية الجاني الفاعل عن نيته تملك مال الغير [(4)].

في حين يرى جانب آخر من الفقه ، ضرورة توافر القصد الخاص، أي نية تملك المال من قبل الفاعل، بحيث يتوجب على الفاعل أن تتجه إرادته إلى تملك مال الغير لنفسه، أو لحساب شخص آخر، بحيث أن الفاعل لو قام بالاستيلاء على المال مثلاً من باب المزاح، ثم قام بإعادته فإننا لا نكون أمام قصد جرمي خاص، تتبلور من خلاله جريمة الاحتيال الإلكتروني، على أنّه لا يعتد بالباعث لدى الفاعل وأنّه لا ينفي عنه قصده الاحتيالي، في ارتكاب الجريمة، كمن قام بهذا الفعل المجرم

---

(1) إبراهيم، حوكمة الإنترنت، ص391.

(2) الشيخني، عبدالقادر، (2009)، جريمة الاحتيال، الطبعة الأولى، منشورات الحلبي، بيروت، لبنان، ص181.

(3) إبراهيم، حوكمة الإنترنت، ص393.

(4) البحر، الجرائم الواقعة على الأموال في قانون العقوبات الإماراتي، ص230.

لاستيفاء دين له، أو بقصد أثبات قدراته في مجال الثورة المعلوماتية، أو كان الباعث لديه الطمع[1].

ومن وجهة نظر الباحث، أنّه وبمجرد توافر العلم بارتكاب هذا النشاط المجرم بالنص القانوني، فإن إرادة الجاني تحققت ما دام أنّه ليس مكرهاً على ذلك، ومدرك لنصاب الأمور من حوله، ويعي العواقب المترتبة على مثل هذا الفعل المجرم، وأن القصد الخاص المتعلق بنية التملك متحققة، بمجرد الاستيلاء على المال، فمن قام بهذا السلوك، واستولى على مالِ الغيرِ بهذه الطريقة، لا يُقبل منه بسهولة، أن يدعي بعدم توافر نية التملك لديه.

(1) الشناوي، جرائم النصب المستحدثة، ص53.

الفصل الثاني

الاحتيال الإلكتروني عن طريق الحاسب الآلي وبطاقات الدفع الإلكتروني

سوف نقسم هذا الفصل إلى أربعة أقسام نخصص الـقسم الأول للحديث عن جرائم الاحتيال الإلكتروني عن طريق الحاسب الآلي، أما الـقسم الثاني، فسوف نتناول فيه جرائم الاحتيال الإلكتروني بواسطة بطاقات الدفع الإلكتروني وأهم المؤسسات العاملة بهذا المجال، في حين نتناول بالـقسم الثالث، كيفية مواجهة جرائم الاحتيال الإلكتروني ببطاقات الدفع الإلكتروني، ونخصص الـقسم الرابع، للحديث عن المواجهة التشريعية لجرائم الاحتيال الإلكتروني في التشريع الأردني.

1.2 جرائم الاحتيال الإلكتروني بواسطة الحاسب الآلي:

إن أجهزة الحاسب الآلي ومن بعد التطور والانتشار، الذي رافق هذه التقنية من بداية عقد الثمانينيات، والإزدياد الملحوظ لتطور هذه التقنية منذ بداية الألفية، جعل منها اداةً يُعتمد عليها في مختلف مجالات الحياة، سيما المتعلقة بالأموال وآلية حفظها بالبنوك، وتحويلها الكترونياً، لما توفره من سرعة ودقة في العمل، لتجعل من أنظار الجناة المحتالين، محَط اهتمام واستغلال لهذه التقنية بصورة غير مشروعة، لارتكاب جرائم الاحتيال الإلكتروني، بالاستخدام غير المشروع لأجهزة الحاسب الآلي، بعد تطويعها والتلاعب بمدخلات ومخرجات البيانات، والمعلومات والبرامج المستخدمة بهذه الأجهزة، بالتستر وراء شاشات هذه الأجهزة بدون مواجهة مباشرة مع المجني عليهم؛ بغية الاستيلاء على أموال الغير[1].

وسوف نتناول هذا الـقسم، من خلال أجزاء متعاقبة نتناول بالـجزء الأول جرائم الاحتيال الإلكتروني من خلال أنظمة الحوالات البنكية الإلكترونية، والـجزء الثاني نخصصه للحديث عن رسائل البريد الإلكترونية الخادعة من خلال شبكة الانترنت.

---

(1) مصطفى، جرائم الحاسبات الآلية في التشريع المصري، ص320.



1.1.2 الاحتيال الإلكتروني من خلال أنظمة الحوالات البنكية الإلكترونية:

إن الاحتيال الإلكتروني من خلال أنظمة الحِوالات البنكيـة، أو مـا يـسمى بالتحويل الإلكتروني للأموال، تُعد مِن أكثر حالات الاحتيال الإلكتروني، التي تقع في أوساط التعاملات البنكية، وذلك من خلال الاعتماد شبة المطلق، على خـدمات الحاسب الآلي داخل هذه التعاملات البنكية؛ بغية استيعاب حجم وحركـة الأمـوال، وهذا الاعتماد بدوره خلق المجال لسلسلة مـن التلاعبـات الماليـة فـي القطـاع المصرفي، والتي غالباً ما تنتهي بـ الاستيلاء على مبالغ مالية كبيرة، فمن هنا، يتوجب علينا معرفة المقصود بالتحويل الإلكتروني للأموال، وكيفية التلاعـب فـي هـذه الأنظمة للأموال إلكترونياً(1).

ويمكن تعريف التحويل الالكتروني للأموال بأنّه : عمليات تبادل لقيم ماليـة، تتم بوسائل إلكترونية عوضاً عَن الوسائل الكتابية، والمقصود هنا بنظـام التحويـل الإلكتروني: ليس التحويل الذي يجري بين البنوك فيما بينها فقط، بل يشمل جميـع المعاملات المالية التي تتم من خلال تبادل ونقل الأموال الكترونياً بعيداً عن الطرق التقليدية واليدوية(2).

وتتبلور الأجزاء الرئيسية للتحويل الإلكتروني للأموال من خلال ما يلي:

(1) الحاسب الآلي المركزي:

وهو المركز الرئيسي، الذي يتم من خلاله معرفة أي تحويل، أو حركـة للأموال، من جميع الأرصدة المالية التابعة لهذا المركز الرئيسي، والذي بـدوره يُحفظ به جميع الملفات الخاصـة بالأرصـدة، والعمـلاء ورجـال الأعمـال والموظفين، وأي حركة حسابية يتوجب أن تمر مـن خـلال الحاسـب الآلـي المركزي(3).

(1) السرحان والمشهداني، أمن الحاسوب والمعلومات، ص113.
(2) ذوابة، محمد عمر، (2006)، عقد التحويل الإلكتروني، الطبعة الأولى، دار الثقافة للنشر، عمان، الأردن، ص22.
(3) قورة، جرائم الحاسب الآلي الاقتصادية، ص497.

(2) نقاط البيع:

هي نهايات طرفية مرتبطة بالحاسب الآلي المركزي، وقد باتت منتشرة في الكثير من متاجر البيع، ومعظم الأماكن التي تعتمد مبدأ البيع والشراء والسرعة في التعامل، ويتم ذلك من خلال البطا قة الممغنطة، وإدخالها في شق وحيز مصمم خصيصاً، يتم من خلاله نقل معلومات البطاقة إلى المركز الرئيسي، بحيث يظهر اسم العميل ورقم حسابه، وكل ما يتعلق بالمعلومات الخاصة لإنجاح هذه الحركة التجارية[1]، وسوف نتطرق إلى هذه العملية، بشكل أكثر تفصيلاً في الأقسام التالية.

(3) أجهزة الصرف الآلي:

إن أجهزة الصرف الآلي، باتت بلا شك منتشرة بشكل غير مسبوق مما كانت عليه سابقاً، وإن هذه الأجهزة بطبيعة الحال، مرتبطة بالحاسب الآلي المركزي، والتي تمكن المستخدم من إجراء عمليات تحويل الكتروني، خصوصاً إن مثل هذه الصرافات الآلية، تقدم خد ماتها على مدار الساعة بلا توقف سواء بالإيداع، أو سحب النقود، وإن كانت هذه المبالغ ذات سقف مالي محدد، ليس كبيراً ليتوافق والغاية التي أنشأت من أجلها هذه الأجهزة[2].

ومما لا شك فيه، إن التحويل الإلكتروني للأموال، قد أسهم في خلق مزايا لا يمكن إنكارها، سواء من خلال السرعة وزيادة الثقة بالتعاملات المالية، والحد من السرقة التي كانت ترافق عمليات التحويل النقدي اليدوي، بالإضافة إلى زيادة حجم المبيعات، بحيث أصبح الكثير من التجار، يرغبون بالعمل من خلال السداد بطريق التحويل الإلكتروني، من أرصدتهم بدلاً من الدفع النقدي ، والذي كان يأخذ وقتاً وجهداً أكثر في إتمامه، وتتم عملية التحويل الإلكتروني من خلال أمر يتلقاه المصرف من قبل مالك الحساب (العميل)[3]، بدون أن يأخذ شكلاً محدداً، بل يكفي معطي الأمر، أن يكون هو مالك الحساب، أو لديه السلطة بالتصرف بهذا الحساب،

---

(1) أبو جريش، جورج؛ ورشوان، خشان يوسف، (2004)، المدخل إلى مصارف الانترنت، الطبعة الأولى، إتحاد المصارف العربية للنشر، بيروت، لبنان، ص176.

(2) أبو شامة، عولمة الجريمة الاقتصادية، ص84.

(3) العريان، الجرائم المعلوماتية، ص127.

ولا تتم عمليةالتحويل، إلا بعد التأكد الكامل من جميع البيانات والمعطيات الخاصة بالعميل، والحساب والمصرف، وتوثيق ذلك بالسنة والشهر واليوم والساعة، بالإضافة إلى وجوب توافر الأهلية، لجميع أطراف العملية المصرفية المالية، وأن آلية التحويل الإلكتروني للأموال، قد تتم إما لكامل الحساب، أو لجزء من المبلغ، وذلك بحسب رغبة مالك الحساب والوسائل الإلكترونية التي يستعملها العميل، والتي تتيح له إجراء عمليات تحويل متعددة ومتنوعة، ولم ترد على سبيل الحصر، لما يدخل عليها من تطور مستمر بما يتناسب وكل فترة زمنية ونذكر من هذه الوسائل[1]:

السحب والإيداع النقدي، وتحريك الحسابات عن بعد، لما تتعرض له الحسابات الجامدة من عمليات احتيالية، وإنشاء واستعمال الشيكات الإلكترونية، وإنشاء واستعمال السندات التجارية، والأوراق المالية الإلكترونية، أما طرق التلاعب في أنظمة التحويل الإلكتروني للأموال، فهي أيضاً قائمة على الابتكار والتجديد، إلى كل ما هو غير متوقع للعميل والبنك ونذكر منها:

(1) التلاعب بالمكونات المادية الخاصة بنظام التحويل الإلكتروني للأموال، وذلك من خلال تغيير، أو تعديل هذه البيانات والتلاعب بها، أو من خلال خلق بيانات جديدة تُزج بالنظام؛ بغيةَ الاستيلاء على هذه الأموال[2].

(2) استعمال البرامج الخاصة بأنظمة التحويل الإلكتروني للأموال، أو إنشاء برامج مطابقة لها، وبالتالي إخفاء البرامج الأصلية، المعدة للنظام الحالي عند استخدام بطاقة شخص لشخص آخر، من أجل سحب مبالغ ماليه دون علم صاحبها الحقيقي[3].

(3) عملية (Perruque): وفيها يتم استقطاع بعض السنتات (الفلسات) من بعض الإيداعات، وتحويلها إلى حسابات أخرى بصورة غير مشروعة، وغير

---

(1) سفر، أحمد، (2008)، أنظمة الدفع الإلكتروني، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، ص66.

(2) Singleton, T., (2010) , Guard Against Gybertheft. Journal of Accountancy. Vol5. p 2.

(3) الطوالبه، الجرائم الإلكترونية، ص187.



مكشوفة، خصوصاً إذا كان النظام البنكـــي، لا يـــستطيع اكتـــشاف المبـــالغ الصغيرة (الفلسات)(1).

(4) عملية (Salami) المتمثلة باستقطاع مبالغ مالية صغيرة من حسابات مالية كبيرة، وتحويلها الكترونياً إلى حساب الشخص المحتال. (2)

وعند ذكر الجرائم المتعلقة بالتحويل الإلكتروني للأموال، يكاد لا يخلو مؤلف من ذكر القضية المشهورة المعروفة باسم (RV.Thompson).

حيث إن المدعو Thompson والذي عين في العام 1979 خبيراً للبرمجيات، في البنك التجاري الكويتي في دولة الكويت، قام بفتح خمسة حسابات فـــي الفـــروع الخمسة داخل البلاد، خلال العام ذاته، وأثناء سفر رئيسه بالبنك، تمكن من الولـــوج إلى عدد من الأرصدة ذات المبالغ الضخمة والأرصدة الجامدة، وبعد أخذ المعلومات الكافية عن هذه الأرصدة استطاع تحويل مبالغ مالية من هذه الأرصدة من الفـــروع الخمسة، ومن باب الأمان لم يقم بعملية التحويل بالشكل الكامل، إلا وهو على مـــتن الطائرة مسافراً إلى المملكة المتحدة ومحو كل دليل على هذه العملية الاحتيالية، ومن ثم قام بفتح أرصدة له دخل المملكة المتحدة، وقام بمخاطبة مدير البنـــك بالكويـــت، مطالباً منه تحويل أمواله الموجودة بالبنك، وقام مدير البنك بتحويل هذه الأموال، بعد التأكد من سلامتها، حيث قدرت هذه الأموال بـــ (45) ألف جنية، وبعد الإنتها مـــن عملية التحويل إلى المملكة المتحدة، تم اكتشاف هذه الجريمة الاحتيالية ليُسارع بعـــد ذلك إلى تقديم هذا المحتال إلى المحاكمة في العام 1983، بتهمة الحـــصول علـــى أموال بطريق الخداع، وحكم عليه بالسجن خمسة عشر شهراً(3).

2.1.2 رسائل البريد الإلكتروني الخادعة:

إن الانترنت، بات يشكل بيئة خصبة لجرائم الاحتيال الإلكتروني، وذلك منـــذ بدايات القرن الحادي والـ عشرين، فلم يعد المجرم المحتـــال، بحاجـــة إلـــى الأدوات

---

(1) سفر، أنظمة الدفع الإلكتروني، ص68.
(2) الشوابكة، جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، ص187.
(3) قورة، جرائم الحاسب الآلي الاقتصادية، ص504 وما بعدها.

والمعدات والتحضيرات، التي تأخذ الكثير من الوقت للقيام بجرمه الاحتيالي، فلقد تكفل الحاسب الآلي، من خلال شبكة الانترنت، بأن يكون هو الأداة ومسرح الجريمة الاحتيالية، سيما مع اعتماد كبرى الدول المتقدمة، على أعما لها من خلال الشبكة الإلكترونية والانترنت، الذي يوفر لها السرعة والدقة في الأعمال على حد سواء، حيث انتشرت في الآونة الأخيرة، ظاهرة متفاقمة ومطردة، بقيام بعض المحتالين بإرسال رسائل مجانية بالبريد الإلكتروني، توهم الضحايا بفرصة الحصول على ملايين الدولارات؛ بغية الاستيلاء على أموالهم[(1)].

فالبريد الالكتروني: وهو ما يطلق علية باللغة الانجليزية (E-mail) أي العنوان الإلكتروني الشخصي الذي يُعين من خلاله مستخدم الانترنت، أو يحدد فيه اسم شركة معينه بذاتها مثال (hamzeh_atef@yahoo.com)، ففي هذا المثال اصبح حمزه عاطف هو اسم المستخدم، و @ رمز تواجده على الشبكة في حين وجود إل yahoo تعني اسم الشركة المضيفة، ومن هنا يصبح هذا البريد صالحاً لتبادل الرسائل الإلكترونية عبر شبكة الانترنت، وحيث أننا نجد اليوم العديد من الشركات المضيفة على الانترنت، ومن أشهرها yahoo،hotmail،gmail وغيرها، التي تتيح للأفراد والشركات من تسجيل عنوان الكتروني لهم بالمجان، وهنا تتم المراسلة بين الجاني والضحية، عبر مراسلات البريد الإلكتروني، دون اتصال أو حتى معرفة مسبقة من خلال اشكال احتيالية متعددة الإقناع، ومن أ شهرها طلب المحتال من الضحية مساعدة في إخراج أموال له من بلد معين غالباً ما يكون إفريقيا، بحيث يطلب من الضحية، بعض المعلومات الشخصية [(2)]، مثل رقم الحساب المصرفي، لتحويل الأموال إليه، مقابل نسبة مغرية قد تصل 50%، من ثم يطلب منه أن يدفع مبلغ معين من أجل إتمام عملية التحويل، واقناعة بضرورة ذلك، وهذا ما يسمى (جرائم الدفعة الأولى) فمن غايات إنشاء البريد الإلكتروني، أنّه يستخدم كمستودع لحفظ الأوراق، والمستندات الخاصة بالشخص، والشركات والمؤسسات، شريطة أن

---

(1) الغثبر، خالد بن سليمان؛ والقحطاني محمد بن عبدالله، (2008)، الاصطياد الإلكتروني، الطبعة الأولى، جامعة الملك سعود، الرياض، السعودية، ص11.

(2) الفيل، الإجرام الإلكتروني، ص18.



يتم تأمين آلية الدخول إليه، باستخدام بـرامج الحمايـة، مثـل التـشفير وكلمـات المرور(password) وغيرها من برامج وسبل الحماية[1].

ومن مزايا هذه الخدمة (البريد الإلكتروني)، أنها تعدت خـدمات كـل مـن الهاتف والفاكس، فالمستخدم لن يضطر إلى مراعاة فروق التوقيـت بـين البلـدان، فضلاً عن قلة التكاليف والسرعة والخصوصية، إذ لايحتاج المرسل، إلى الطوابـع، أو الأوراق، أو دفع تكاليف إرسال الرسائل، أو الفاكس[2]، ولكـي يـنعم مـستخدم الانترنت في خدمة البريد الإلكتروني بشكل مثالي، يطلب منه من المعلومات ما يلي:

(1) اسم مزود إرسال البريد الإلكتروني، ويرمز إليه بالرمز (csmtp) وهو المزود المسؤول عن تنظيم عمليات رسائل البريد الإلكتروني، مـن المرسـل إلـى الآخرين.

(2) اسم مزود استقبال البريد الإلكتروني، ويرمز له (pop)، وهو المسؤول عـن استقبال الرسائل من الآخرين إلى بريد المستخدم.

(3) العنوان البريدي الذي تمنحه الشركة المضيفة، أي مقدمة الخدمة للمستخدم إذ يستطيع شخص مقيم بالأردن مثلاً، من مراسلة شخص مقيم بمـصر بثـوان معدودة، ومن دون معرفة مسبقة بينهما، ومن هنا وبوجود مثل هذه المزايـا، تخلق الثغرات للاستخدام غير المشروع، لتوفير البيئة الاحتيالية المناسبة، لمـا يسمى برسائل البريد الإلكتروني الخادعة[3]، وكما ظـاهر لـدينا أن جـرائم الاحتيال الإلكتروني، المرتكبة بواسطة البريد الإلكتروني باتت تمتـاز عـن غيرها من جرائم الاحتيال التقليدية، من حيث الشكل والأسلوب وآلية ارتكاب الجرم، حيث أن هذه الجرائم، ترتكب باستخدام شبكة الانترنت، على خـلاف

---

(1) حجازي، علم الجريمة والمجرم المعلوماتي، ص55 .

(2) ابراهيم، حوكمة الإنترنت، ص96، 97.

(3) Kunz, M. & Wilson, p., (2004) , "Computer Crime and fraud", Report to the Montgomery County Criminal Justice Coordinating Commission, p 13.

جرائم الاحتيال التقليدية، التي تكاد لا تحصر اشكالها وقابليتها لـ لابتكار والتجديد، وهي أوسع وأعمّ منها لدى جرائم البريد الإلكتروني الاحتيالية(1).

ومن أهم ما يميز جرائم الاحتيال بواسطة البريد الإلكتروني، أنّها تتم بين أشخاص متباعدين عن بعضهم البعض جغرافياً، أي أنها عابرة للحدود، على عكس جرائم الاحتيال التقليدية، التي تقع غالباً بين الجاني أو اتباعه، وبين المجني عليهم نتيجة التعامل المباشر وجهاً لوجه، ويميز هذه الجرائم المرتكبة عبر البريد الإلكتروني، عن غيرها من الجرائم المعلوماتية بشكلها العام؛ أنّه لا يمكن أن تتم جرائم الاحتيال عبر البريد الإلكتروني، بدون توافر خدمة الانترنت، في حين إمكانية وقوع الجرائم المعلوماتية، بدون توافر لهذه الخدمة، ونلاحظ اشتمال جرائم البريد الإلكتروني في محل الجريمة، على المال المنقول المادي والمعنوي على حد سواء، في حين أن الجرائم المعلوماتية، غالباً ما يقتصر محل الجريمة فيها، على المال المعنوي، والمقصود به: البيانات والمعلومات المخزنة وليس المال المادي(2).

أما القصد الجنائي الخاص، فنجد أنّه في جرائم الاحتيال بواسطة البريد الإلكتروني، يتمثل بنية الاستيلاء على مال الغير، بينما في الجريمة المعلوماتية، يتمثل القصد الجنائي الخاص بها من خلال التلاعب بالبيانات، والمعلومات والمعطيات المخزنة داخل أجهزة الحاسب الآلي، لذلك لابد لنا من الاعتراف بخصوصية مثل هذا النوع من الجرائم، وما يميزها عن غيرها من الجرائم، ووضع الآلية التشريعية اللازمة لمواجهتها(3).

ومن أهم صور الاحتيال عبر رسائل البريد الإلكتروني:

(أ) قيام إحدى الجهات بإرسال رسالة الكترونية، إلى عدد غير محدود وكبير من مستخدمي خدمة البريد الإلكتروني، من خلال جهاز إرسال خاص لهذه الغاية، يكتب فيها على سبيل المثال، كلمة مبروك لكي تجلب حماس القارئ، تُبين أنّك

---

(1) رباح، غسان، (2008)، الوجيز في قضايا الملكية الفكرية والفنية مقارنة مع الجريمة المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، ص112.

(2) الغثبر والقحطاني، الاصطياد الإلكتروني، ص196.

(3) الفيل، الإجرام الإلكتروني، ص21.

ربحت مبلغ مليون دولار أميركي، من خلال شركة يا نصيب تختار الرابحين بصورة عشوائية من مستخدمي الشبكة، بحيث يذكر في متن الرسالة الإلكترونية، أن هذه الشركة قد وجدت ومنذ فترة مبلغاً نقدياً كبير يقدر بملايين الدولارات، يتبع لحساب أحد زبائنها، الذي توفي هو وجميع أفراد عائلته، في حادث تحطم طائرة ومنذ ذلك الوقت لم يتقدم أحد من أقاربه للمطالبة بهذه الأموال، وتأكدت الشركة من عدم وجود أي وريث شرعي، فقررت أن تعمل على إرسال هذه الأموال، إلى عدد من الأشخاص المحظوظين، من مستخدمي هذه الشركة باليانصيب، وقد وقع الاختيار عليك، من أجل ذلك، نطلبك بتزويدنا بما يلي : رقم حسابك المصرفي، اسم البنك المتعامل معه، رقم الهاتف، وعندما يقوم الضحية بالرد، ترده بعد ذلك رسالة تأكد ربحه المبلغ، من ثم يطلب منه أن يدفع مبلغ من المال، من أجل إجراء عملية تحويل الأموال، وبعد قيام الضحية بذلك، تنقطع المراسلة ولا يأتي أي رد من المحتالين[1].

(ب) قد يأتي الا حتيال عبر البريد الإلكتروني، من خلال انتحال أحد الأشخاص، صفة موظف لدى إحدى الشركات العاملة بمجال إدارة شبكة الانترنت، خصوصاً المشهورة منها، وسوف نذكر هذه الواقعة لرسالة بريدية إلكترونية، تم إرسالها من قبل شخص، ادعى أنّه موظف لدى شركة ياهو، حيث يطلب من المستخدمين، إرسال بياناتهم من أجل الحصول على جائزة مالية.

"شكراً لمساهمتكم في نجاحنا

(1) عاطف، زياد، (د.ت)، الاحتيال الإلكتروني من مشكلة إلى أزمة، متوفر عبر الموقع: www.coeia.edu.sa، تجدر الإشارة إلى أن تقنيات الويب التي تطلق على شبكة الانترنت العالمية (www)، هي اختصار لكلمة (word wide web) وهي أكثر الأنظمة انتشاراً وشهرة على الانترنت في مجال البحث عن المعلومات والاتصال، فهي نظام عالي الكفاءة، حيث يقوم بربط الوثائق الإلكترونية عبر الآلاف من أجهزة الحاسب الآلي عبر الشبكة، وتقدم الخدمة من خلال النصوص الكتابية والصورة والصوت والفيديو. للمزيد حول ذلك انظر العبودي، تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني، ص31.

يسرنا إبلاغك عن نتيجة الإعلان، والدعم المالي الذي عقدته yahoo هذه السنة، حيث فاز موقعك الإلكتروني، المرفق معه رقم التذكرة (88373457492) مع الرقم التسلسلي (7263.263) ورقم الدفعة (8254297137) يانصيب مرجع رقم (336065782) ورقم الحظ الرابح (142228374044) وهو الرقم الفائز بالجائزة النقدية من الفئة الأولى، لذلك وقع عليك الاختيار للحصول على مبلغ (1000,000) جنيه إسترليني، وللمطالبة بالجائزة النقدية، يرجى الاتصال بمدير قسم المطالبات، سيد كريستوفر جيمس والكر في المملكة المتحدة.

سيد كريستوفر جيمس والكر

مدير إعلانات الياهو في المملكة المتحدة

ياهو المملكة المتحدة xxxxxxx

عنوان البريد الإلكترونيxxxxxx@ADVIRE.COM

هاتف xxxxxxx

لتجهيز وتحويل الأموال، الرجاء تزويدنا بالبيانات التالية :الاسم الكامل، البلد، عنوان الاتصال، الجنس، العمر، العمل، رقم الهاتف.

تهانينا الحارة مرة أخرى من كل موظفي ياهو.

لكم خالص الشكر

سيده اميليا هانت" انتهت الواقعة التوضيحية[1].

وفيما يلي قائمة بأسماء أول عشرة دول، من حيث احتضانها لمواقع الاحتيال عبر البريد الإلكتروني:

(1) الحيط، عادل عزام سقف، (2011)، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية، الطبعة الأولى، دار الثقافة للنشر، عمان، الأردن، ص151وما بعدها.

الجدول رقم (1)

أول عشرة دول من حيث احتضانها لمواقع الاحتيال

الرقم	الدولة	النسبة (%)
1	الصين	24,21
2	الولايات المتحدة الأمريكية	23,85
3	الهند	9,39
4	روسيا	8,06
5	تايلند	4,64
6	رومانيا	3,53
7	المانيا	3,41
8	كوريا الجنوبية	2,42
9	بريطانيا	1,47
10	فرنسا	1,27

وكما نلاحظ، أن معظم هذه الدول، تُعد ممن ساهموا في نشر وازدهار تكنولوجيا المعلومات، وتمتلك القدر الكافي من الخبرة الإلكترونية، وتطويرها على الصعيد العالمي[1].

وبحسب رأي الباحث، إنّ تصّدر هذه الدول في احتضانها لمواقع الاحتيال عبر البريد الإلكتروني، غير مقتصر لكونها من الدول التي ساهمت في إزدهار هذه التكنولوجيا وابتكارها العديد من الوسائل الاحتيالية فقط، بل أيضاً بسبب تعدادها السكاني الكبير، مقارنةً مع غيرها من الدول، وهذا ما تبينه الإحصائية في تربع كل من الصين، والولايات المتحدة الأمريكية، والهند على المراتب الثلاثة الأولى.

(1) الغثبر والقحطاني، الاصطياد الإلكتروني، ص56.

2.2 جرائم الاحتيال الإلكتروني بواسطة بطاقات الدفع الإلكتروني

إنّ المنظومة الإلكترونية، باتت شديدة التشعب والتعقيد، والتأثير في حياة الأفرادفي الحاضر والمستقبل ، بحيث يصعب التنبوبما سوف يسفر عنها من تطورات متلاحقة، حيث أصبحتعنصراً ضرورياً في الواقع الملموس ، لتطل علينا بطاقات الدفع الإلكترونيبنشاط تكنولوجي واسع الانتشار ، وإنْ كان هذا النوع من التقنية الإلكترونية،بات لا يخلو من مخاطر الاستعمال غير المشروع ، ووضع العراقيل والتحديات في الاستخدام الآمن لمزايا هذه البطاقات الإلكترونية، التي أصبحت من أكثر صور جرائم الاحتيال الإلكتروني، على المستوى الدولي، خصوصاً إنْ مميزاتاستعمال هذه البطاقات ، أصبحتضرورة ملحة ، تعكس السرعة والدقة والسهولةفي تعاملات مستخدميهافي الكثير من مناحي الحياة الاقتصادية والاجتماعية[1]، وعليه سوف نتناول في هذا القسم، نشأة وتطور بطاقات الدفع الإلكتروني من خلال الجزء الأول، والجزء الثاني، نتناول فيه أطراف العملية التجارية لبطاقات الدفع الإلكتروني، في حين نفرد الجزء الثالث، للحديث عن أهم أنماط الاعتداء على بطاقات الدفع الإلكتروني.

1.2.2 نشأة وتطور بطاقات الدفع الإلكتروني:

بطاقة الدفع الالكتروني : هي عبارة عن بطاقة بلاستيكية، صادرة عن مؤسسة مالية ما، تُمنح للعملاء بحيث تسمح لهم إجراء معاملات مالية، تتمثل بدفع قيمة الخدمات، أو المشتريات التي يحصلون عليها، أو سحب مبالغ مالية نقدية من حساباتهم، وفقاً لشروط فنية وقانونية، خاصة بكل نوع من أنواع هذه البطاقات الإلكترونية، فهي إذاً أداة تقوم مقام النقود بالتعاملات ولا يتم إبطالها، أو إقرار انتهاء صلاحيتها، إلا من قبل الجهة المصدرة لها[2]، وكانت بدايات هذه البطاقة، في العام 1949 عندما كان السيد مكنمار، والذي يعد من أحد كبار العاملين بالبنوك الأمريكية، جالساً في أحد المطاعم، وعندما حصل على فاتورة الغذاء كانت باهظة

---

(1) سفر، أنظمة الدفع الإلكتروني، ص9.

(2) الملط، الجرائم المعلوماتية، ص193.

الثمن، ولم يكن معه من المال ما يكفي لسداد قيمة الفاتورة، مما دفع به إلى الاتصال بزوجته لتجلب له النقود من المنزل لسداد قيمة الفاتورة، ومن هنا بدأت تراوده فكرة بطاقات الدفع الإلكتروني، لتجنب مثل هذه المواقف، فهو الذي أنشأ مؤسسة داينـــزر كلوب، بمساعدة اثنين من رجال البنوك المختصين في العمليات المصرفية، بحيـــث أصدرت هذه المؤسسة، أول بطاقة دفع في العام 1950 إلى 200 عـــضو، حيـــث كانت معتمدة لدى 27 مطعماً، ولاقت الفكرة رواجاً بين المواطنين، ليـــصل عـــدد المستخدمين حتى نهاية العام حوالي العشرين ألف[1].

وفي العام،1958 قامت شركة أميركية تعمل في مجال الخدمات المالية من إصدار بطاقة دفع خاصة بعملائها، وتبعها بالعام ذاته بنك أوف أميركـــا، وأصـــدر بطاقة ائتمان سميت بطاقة أمريكارد، أما في العام 1967، قامت مؤسسة دي لارو، بإنتاج أول ماكينة صرف نقود آلي لبنك باركيز الانجليزي، في حين ظهـــرت أول ماكينة صرف نقود (ATM)، تعمل من خلال شبكات الاتـــصال مـــستخدمة آنـــذاك للبطاقات البلاستيكية، ذات الشريط الممغنط في العام 1972، بينما جاء العام 1973 بطفرة في عالم بطاقات الدفع الإلكترونية، حيث قامت مؤسسة أمريكـــارد، والتـــي أصبحت فيما بعد مؤسسة فيزا العالمية (VISA) بتأسيس أول نظام الكتروني، يعمل علية بطاقات الدفع الإلكتروني، حيث أدى استخدام هذا النظام، إلى التقليل من الـ وقت المستخدم في إجراء المعاملات من خلال هذه البطاقات من خمسة دقـــائق إلـــى 56 ثانية[2]، واستطاع هذا البنك خلال ذلك العام من توفير 30 مليـــون دولار، بفـــضل استخدام هذه البطاقات، في حين كان متجر (Gepehne)، أول من اعتمد مثـــل هـــذه البطاقات للوفاء بقيمة الفواتير، حيث ذاع صيت هذا المتجر، وارتفع حجم مبيعاتـــه، وزادت نسبة الإرباح فيه عما كانت عليه سابقاً، وفي العـــام 1976، أُصـــدرت أول

---

(1) القضماني، حسين إبراهيم، (2002)، البطاقة المصرفية والانترنت، الطبعة الأولى، اتحاد المصارف العربية للنشر، بيروت، لبنان، ص23.

(2) فوزي، نجاح محمد، (2007)، وعي المواطن العربي تجاه جرائم الاحتيال "بطاقات الدفع الإلكتروني نموذجاً"، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، ص56 وما بعدها.

بطاقة دفع الكتروني تحمل شعار (VISA) بعد تحول بنك أمريكارد إلى مؤسسة فيزا الدولية، وتحول بطاقة دفع ماستر التي أنتجت في العام 1966 لتصبح ماستر كـــارد العالمية في العام 1979، وسعتْ هذه المؤسسات المالية، في العام 1984، إلى جعل استخدام هذه البطاقات على النطاق العالمي، من خلال تأسيس ونـــشر نقـــاط قبـــول لبطاقات الدفع الإلكتروني، لتعلن عن ولادة عصر جـ ديد من هذه البطاقات، وبطاقات ماكينة الصرف الآلي خلال عقد الثمانينات والتسعينات، لتدخل عقد الألفية، وقد باتت ضرورة ملحة في تعامل الشركات والأفراد[1].

أما إذا نظرنا إلى بطاقة الدفع الإلكتروني، من ناحية الوصف الشكلي لهـــذه البطاقة، فإننا نجد أنها عبارة عن قطعـ ـة مصنوعة من البلاســـتك، ذات مواصـــفات كيميائية محددة التركيب، ذات أبعاد قياسية محدد ة بطول 85,6 مـــم، فـــي عـــرض 35,9 مم، في حين يبلغ سُمْك هذه البطاقة البلاستيكية 0,76 مم، يدون عليها جميـــع البيانات اللازمة، بحيث يكون جزء من هذه البيانات مرئي، في حـــين يـــتم تـــدوين الجزء المتبقي للبيانات بشكل غير مرئي (مشفر)، على أن يُعطى صاحب البطاقـــة، رقماً سرياً يحتفظ به لنفسه فقط، لكي يتمكن خلاله من استخدام مميزات هذه البطاقة في الأوساط المصرفية والتجارية، وبما أن هذه البطاقات تصدر من قبل مؤســـسات مالية دولية، ذات سمعة وثقة عالية، فالعملاء يسارعون إلى طلب هـــذه البطاقـــات ويثقون باستعمالها، أما من الناحية المصرفية، فهي أداة وفاء معترف بها، ومقبولـــة على نطاق محلي ودولي واسع، لدى الكثير من البنوك، والتجار والأفـــراد كبـــديل للنقود، لدفع قيمة السلع والخدمات، مقابل توقيع حامل البطاقة (العميل) على إيصال قيمة التزامه الناشئ عن شراء السلع أو الاستفادة من الخدمات، من خلال نقاط البيع المختلفة، من ثُمّ يقوم التاجر بالرجوع على البنك، لتحصيل قيمة النقـــود مـــن بعـــد تعاقده المسبق مع هذا البنك[2]، وهذا ما سنبينه لاحقاً.

ومن أهم المؤسسات المالية في مجال بطاقات الدفع الإلكتروني:

---

(1) أبو شامة، عولمة الجريمة الاقتصادية، ص58 .

(2) الفوزان، صالح بن محمد، (2011)، البطاقة الائتمانية تعريفها وأخذ الرسوم على إصدارها والسحب النقدي بها، متوفر عبر الموقع: www.saaid.net/fatwa.

(1) مؤسسة فيزا الدولية ومقرها الرئيسي الولايات المتحدة الأمريكية، لوس انجلوس.
(2) مؤسسة ماستركارد العالمية ومقرها الولايات المتحدة الأمريكية، سانت لويس، نيويورك.
(3) مؤسسة أميركان اكسبرس ومقرها الولايات المتحدة الأميركية.
(4) مؤسسة دانيزر كلوب الدولية.
(5) مؤسسة JCB الدولية ومقرها الرئيسي اليابان[1].

2.2.2 أطراف العملية التجارية لبطاقات الدفع الإلكتروني وأنواعها

إن إصدار البنوك لبطاقات الدفع الإلكتروني جاء في ظل سعيها لتقديم الأفضل لعملائها، وبالنظر إلى أطراف هذه الحركة المصرفية التجارية، فأننا نكون أمام ثلاثة أطراف للعملية التجارية الخاصة ببطاقات الدفع الإلكتروني، ونوعين من أهم أنواع هذه البطاقات.

أولاً: أطراف العملية التجارية

(1) البنك المصدر(Issuer Bank): وهو البنك الذي يعمل على التعاقد مع المنظمات الدولية والتي يهدف من خلالها إلى إصدار البطاقات لعملاء البنك والاتفاق والتعاقد مع التجار، من أجل اعتماد هذه البطاقات كأداة وفاء لديها ويكون من حق البنك إصدار بطاقة تحمل رقماً خاصاً به (PIN)، لكي يتمكن من التواصل مع باقي البنوك الأعضاء بحرية وتعاون مشترك، وقدر كافي من الخصوصية والأمان بذات الوقت، وهذه الـ مؤسسات الدولية، وغالباً ما يتكون هذا الرقم من ثمانية أرقام مطبوعة على سطح البطاقة ابتداءً من اليسار[2].

---

(1) فوزي، وعي المواطن العربي تجاه جرائم الاحتيال "بطاقات الدفع الإلكتروني نموذجاً"، ص62.
(2) السقا، إيهاب فوزي، (2007)، الحماية الجنائية والأمنية لبطاقات الائتمان، الطبعة الأولى، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، ص51.

(2) العميل حامل البطاقة (Card Holder): وهو الشخص الذي يصدر البنك البطاقة باسمه، لكي يتمكن من استعمالها والانتفاع بمميزاتها، مع التزامه بكامل المستحقات الما ية المترتبة على استخدامه للبطاقة، كما أن هذه البطاقة، تصدر للشخص الطبيعي، فهي من الممكن أن تصدر أيضاً باسم شخص معنوي، ويحق لكلاهما، أن يخول شخص ثالث باستخدام هذه البطاقة، مع بقاء الشخص الذي صدرت باسمة البطاقة، هو المسؤول بكافة التزامات البطاقة أمام البا نك المصدر، وذلك بعد طلب يقدمه العميل للبنك، يطلب فيه رغبته في استصدار بطاقة باسمة، ويوّقع على ذلك بعدما يتأكد البنك، من جميع الضمانات والشروط اللازمة لإصدار البطاقة لهذا العميل، مع التزام العميل، بكل شروط العقد الموقعة مع البنك المصدر [(1)].

(3) التاجر (Merchant or Retailer) وهو الجهة التي بدورها تقبل التعامل ببطاقات الدفع الإلكتروني كأداة وفاء، بحيث يوفر التاجر السلع والخدمات، التي يرغب العميل بها، مستخدم البطاقة مقابل أن يقوم العميل بالتوقيع على "إشعار البيع" عند حصوله على هذه السلع أو الخدمات، ويتم ذلك بعدما يكون التاجر، قد تعاقد مسبقاً مع البنك المصدر من خلال عقد أُبرم بينهما، بحيث يقدم التاجر السلع والخدمات لحامل البطاقة، من ثم يقوم البنك بسداد قيمة هذه الإشعارات، بعد تقديمها من قبل التاجر [(2)]، على أن يقوم البنك بتزويد التاجر، ببعض الأدوات اللازمة لإتمام هذه العملية الإلكترونية، ونذكر منها:

(أ) وضع الملصقات والنشرات بباب المحل (المتجر)، لكي يتسنى للعملاء معرفة تعامل هذا المتجر بالبطاقات.

---

(1) غنام، شريف محمد، (2007)، محفظة النقود الإلكترونية رؤية مستقبلية، الطبعة الأولى، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، ص36.

(2) فوزي، وعي المواطن العربي تجاه جرائم الاحتيال "بطاقات الدفع الإلكتروني نموذجاً"، ص59.

(ب) نقاط البيع الإلكترونية (p.o.s) أو ما تسمى وحدة الاتصال الطرفية، والتي يتم من خلالها تمرير البطاقة، والتي بدورها تقرأ البيانات المدونة على هذه البطاقة من خلال الشريط الممغنط.

(ج) آلة طباعة صغيرة الحجم، تستعمل في حالة تعطل نقطة البيع الإلكترونية؛ وذلك للحفاظ على سريان تقديم الخدمة.

(د) تزويد التاجر بإشعارات البيع، التي تم ختمها مسبقاً، من قبل البنك المصدر، التي تخرجها نقطة البيع الإلكترونية[1].

ثانياً: أنواع بطاقات الدفع الإلكتروني

وسوف نُخصص الحديث، عن أشهر نوعين من البطاقات الممغنطة، وهما بطاقة الائتمان، وبطاقة الخصم.

(1) بطاقة الائتمان (Credit Card):

وتعمل هذه البطاقة من خلال نظام الاقتراض من البنك، من خلال سقف ائتماني يحدد سلفاً للعميل، عند استصدار البطاقة الائتمانية، فيحق للعميل سحب هذه النقود، أو استخدمها للوفاء مقابل السلع، أو الخدمات، في حين يحدد السقف الائتماني، وفقاً للضمانات والشروط المتفق عليها بين الطرفين، قبيل إصدار البطاقة وبحسب نشاط ومكانة العميل التجارية، ومنذ صدور البطاقة فإنّه يحق لصاحبها أن يستخدمها مباشرة، إما من خلال البنك نفسه، أو من خلال نقاط البيع الموزعة على المتاجر، ومكاتب الخدمات كبديل للدفع النقدي [2]، هذا ونجد أن معظم البنوك المصدرة للبطاقات الائتمانية، غالباً ما تعطي العميل فترة سماح، قبل البدء بعملية السداد تتراوح بين 30 و 50، يوم في بادرة لتشجيع العملاء لاستخدام هذه البطاقات، وفي نهاية كل شهر، يقوم البنك المصدر بإرسال كشف حساب إلى العميل، متضمن كل المعاملات المالية، التي استخدمها من خلال البطاقة ليتولى العميل بدوره السداد بحسب نسبة الاقتطاع المتفق عليها مع البنك، مضافاً إليها نسبة الفائدة النقدية

---

(1) الرومي، محمد أمين، (2004)، التعاقد الالكتروني عبر الانترنت، الطبعة الأولى، دار المطبوعات الجامعية للنشر، الإسكندرية، مصر، ص130.

(2) أبو جريش ورشوان، المدخل إلى مصارف الانترنت، ص184.

المقررة، على حجم السقف الائتماني، وفي حالة تأخر العميل بالسداد، فإنّ البنك يقوم بترتيب فوائد إضافية، على مبلغ البطاقة الائتمانية من بعد تحذير العميل بوجوب السداد، وإنْ كانتْ بعض البنوك تسعى إلى التفاوض، والحل الود ي؛ بغية استمرار العلاقة التعاقدية مع البنك، من خلال تجديد السقف الائتماني[1].

(2) بطاقة الخصم: (Switch Card)

إنّ بطاقة الخصم، تشكل النسبة الأكبر في العالم، من حيث مستخدمي هذه البطاقة، فقد بينت الدراسات، أن ربع سكان العالم يستخدمون بطاقة الخصم، فهي توفر لهم ال كثير من الراحة والسرعة، فإذا نظرنا إلى هذه البطاقة، من ناحية الشكل، نجد أنّه لا فرق بينها وبين بطاقة الائتمان، فكلاهما بطاقات بلاستيكية، تحمل معلومات وبيانات الحساب والعميل، وكلاهما يستخدمان كبديل للنقود، ولكن يتضح الفرق بينهما، من خلال الاسم الذي تحمله كل بطاقة، فبطاقة الائتمان تعني، الاقتراض من البنك، في حين بطاقة الخصم تعني، الرصيد الفعلي الخاص بالعميل وليس البنك، وهذا يدلنا إلى أن بطاقة الائتمان تتيح لصاحبها السداد فيما بعد، بينما بطاقة الخصم توجب الدفع الفوري للعميل من رصيده، ما لم يكون هنالك أي مخالفة لشروط الاستخدام[2]، بمعنى ارتباط بطاقة الخصم وبشكل مباشر بالحساب البنكي لصاحبها فإنّه في هذا الحالة، يستخدم رصيد حسابه الشخصي وليس الاقتراض من قبل البنك، ومن باب التعريف أكثر بطبيعة المعلومات المدونة على هذه البطاقات، نذكر أركان البطاقة الأساسية الثابتة الغير قابلة للتغير:

---

(1) الدبيان، دبيان محمد، (2011)، بطاقات الائتمان والتكييف الفقهي، متوفر عبر الموقع: www.alukah.net.

(2) قورة، جرائم الحاسب الآلي الاقتصادية، ص509. تجدر الإشارة إلى أن البعض تناول أنواعاً أخرى من البطاقات، وإن كانت تعتبر إما من بطاقات الائتمان، أو بطاقات الخصم، مثل بطاقة الدفع المؤجل، وهي من البطاقات غير المنتشرة، وتدخل تحت مظلة بطاقات الخصم، ومن البطاقات أيضاً، بطاقة ضمان الشيكات، وهي كذلك من البطاقات التي تتدرج تحت بطاقات الخصم، لارتباطها برصيد صاحبها. فوزي، وعي المواطن العربي تجاه جرائم الاحتيال"بطاقات الدفع الإلكتروني نموذجاً، ص68.

(1) رقم البطاقة: وهو الرقم الذي طبع على البطاقة والمسجل لدى البنك المصدر، والمكون من ستة عشر رقماً.
(2) اسم حامل البطاقة : وهو اسم طالب البطاقة من قبل البنك المصدر، والمستخدم والحامل الشرعي لها.
(3) تاريخ إصدار البطاقةأي الشهر الذي أصدرت فيه البطاقة، وهو التاريخ الذي يبدأ منه سريان صلاحية البطاقة للاستخدام.
(4) تاريخ الصلاحية: وهو الذي يحدد الشهر الذي تنتهي به صلاحية استخدام البطاقة، والذي لا يجوز التعامل بها بعد هذا التاريخ.
(5) اسم البنك المصدر : وهو البنك الذي سُمح له بإصدار هذه البطاقة، ويحمل اسم البنك وشعاره[1].
(6) شعار الهيئة الدولية : وهو شعار المنظمة، أو المؤسسة الدولية المصدرة للبطاقة، بغض النظر عن البنك المصدر.
(7) الشريط الممغنط: الذي يحتوي وبشكل غير مرئي على البيانات والمعلومات، الخاصة بالعميل والحساب والبنك.
(8) الصورة الحسية ثلاثية الأبعاد (هولوجرام): وهي إحدى العلامات الأمنية المميزة، التي تُظهر صورة ثلاثية الأبعاد عند تحريكها، شبيهة بالمطبوعة على النقود الورقية.
(9) الرقم السري: وهو غير مرئي، حيث يحفظه العميل لكي يتمكن من الاستخدام الآمن للبطاقة[2].

3.2.2 أهم أنماط الاعتداء على بطاقات الائتمان

تبلورت فكرة تطبيق استخدام بطاقات الدفع الإلكتروني بأنواعها؛ بغيَة تسهيل عملية تبادل ونقل النقود والاستفادة من الخدمات، إلا أنّه يتوجب أنْ يُشارَ إلى

---

(1) البغدادي، كميت طالب، (2008)، الاستخدام غير المشروع لبطاقة الائتمان، الطبعة الأولى، دار الثقافة للنشر، عمان، الأردن، ص65.
(2) السقا، الحماية الجنائية والأمنية لبطاقة الائتمان، ص58 وما بعدها.

الاستخدام غير المشروع لهذه البطاقات الإلكترونية، كأحد صور جـرائم الاعتـداء على بطاقات الدفع، والتي باتت أحدى أبرز جرائم الاحتيال الإلكتروني [1]، وغالباً ما تأخذ هذه الاعتداءات الصور الآتية:

(1) إساءة استعمال بطاقة الائتمان من قبل صاحبها : وتتمثل هذه الحالـة، فـي محاولة حامل البطاقة الشرعي، من ابتكار وسائل واساليب احتيالية يستخدمها للاستفادة من بطاقته الائتمانية، مع تحلله من الالتزامات الماليـة والقانونيـة المترتبة عليه، جراء استخدامه البطاقة [2]، وتتمثل هذه الأساليب من خـلال عدة صور نذكر منها ما يلي:

أ. الاعتداء بالحصول على بطاقة ائتمانية بمستندات مزورة : بحيث يلجأ طالـب البطاقة، إلى تقدم مستندات، وبيانات، وضمانات مزوره، عند إصدار البطاقة التي يطلبها البنك، وعند الانتهاء من استخدام البطاقة، يختفي هذا العميل، ولا يتمكن البنك من الوصول إليه، أو إثبات ذلك؛ لأن المعلومات التي لديـة لا تدل على حقيقة هذا العميل[3].

ب. إساءة استعمال البطاقة بعد انتهاء صلاحيتها : الأصل أن العقد المبـرم بـين العميل والبنك، يوجب العميل أن يسلم البطاقة المنتهية للبنك، وتتمثـل هـذه الحالة، بامتناع العميل عن تسليم البطاقة، في محاولة منـه لابتكـار طـرق احتيالية للاستيلاء على مال الغير من أرصدتهم، وذلك في حال تمكنـه مـن التحايل على ماكينة الصراف الآلي[4].

ج. إساءة استعمال البطاقة رغم إلغائها من المصدر : وتتمثل هذه الحالة، بإلغـاء البطاقة من قبل البنك المصدر، ومع ذلك يقوم حامل البطاقة بابتكار بعـض الوسائل الاحتيالية لاستخدام البطاقة.

---

(1) البغدادي، الاستخدام غير المشروع لبطاقة الائتمان، ص15.
(2) قورة، جرائم الحاسب الآلي الاقتصادية، ص522.
(3) القضماني، البطاقة المصرفية والانترنت، ص124 .
(4) الزعبي، جلال محمد؛ والمناعسة، أسامة أحمد، (2010)، جرائم تقنية نظم المعلومات الإلكترونية، الطبعة الأولى، دار الثقافة للنشر، عمان، الأردن، ص207.

د.إساءة استعمال البطاقة بتجاوز حد السحب المقرر : بحيث يسمح حامل البطاقة لنفسه، من تجاوز سقفه الائتماني بصورة احتيالية، بدون موافقة البنك، وغالباً ما تتم هذه الحالة، من خلال التواطىء مع أحد الموظفين العاملين بالبنك[1].

(2) الاعتداء على نظام بطاقة الائتمان من خلال التاجر : ويتم ذلك من خلال عدة صور، ولكن أكثرها استخداماً، عندما يقوم التاجر بإقناع حامل البطاقة، بأنه يتوجب عليه أن يقوم بتمرير البطاقة، أكثر من مرة بجهاز نقاط البيع p.o.s، بحُجة وجود عطل ما بالجهاز، واستصدار إشعار العميل بالإضافة إلى إشعار آخر فارغ ، ليسارع بعدها التاجر بتعبئة هذه الإشعارات الفارغة، والمطالبة بقيمتها من البنك، بعد ما قلد توقيع صاحب البطاقة من خلال الإشعار الأصلي[2].

(3) الاعتداء على نظام بطاقة الائتمان من قبل الغير : والمقصود بالغير: من هم خارج نطاق العملية التجارية، التي تجمع العميل والبنك والتاجر، وتتخذ هذه الصورة عدة أشكال ومنها:

(أ) تزوير البطاقة الائتمانية بحيث يتمكن الشخص من الحصول على بطاقة العميل بصورةً أو بأخرى، سواء بالاحتفاظ بها لفترة معينة، أو أنهّا فقدت من صاحبها[3]، فيقوم بنسخ البيانات الموجودة على الشريط الممغنط لهذه البطاقة الأصلية، على بطاقة أخرى قلدت لهذه الغاية، وتسمى هذه الصورة (Skimming Devise) وقد تتم عملية التزوير في الغالب، من خلال بعض العصابات المنظمة، التي تحصل على بيانات البطاقات والأرقام السرية، من خلال تركيب جهاز نسخ على مكان إدخال البطاقة في أجهزة الصرف الآلي، مزود بكاميرا صغيرة تقوم بنسخ الأرقام السرية، لكل بطاقة تم استخدامها، من

---

(1) زين الدين، جرائم نظم المعالجة الآلية للبيانات، ص146.

(2) البغدادي، الاستخدام غير المشروع لبطاقة الائتمان، ص175.

(3) العبدان، روان عبدالرحمن، (2011)، تطبيقات آمنه في عمليات الدفع الإلكتروني، متوفر عبر الموقع: www.coeia.edu.sa.

ثم يشرع هؤلاء المحتالين، باستخدام هذه الأرقام والاستيلاء على أموال الغير، دون أدنى معرفة بينهم[1].

(ب) اعتداء الغير بالاحتيال للاستيلاء على أموال بطاقات الائتمان: بحيث يحصل المحتالون، على بيانات هذه البطاقة، ويستخدموها من خلال بطاقات مقلدة، بدون علم أصحابها بوسائل احتيالية، علماً أن البطاقة الأصلية مع حاملها الشرعي، كأن يتواطئ المحتال مع التاجر، من خلال تزويده ببيانات البطاقة، من خلال إشعارات الشراء، بعد التلاعب بها ويتقاسما المال معاً، أو من خلال انتحال المحتال، شخصية موظف البنك، ويتصل بحامل البطاقة، ويطلب البيانات منه بحجة تحديث النظام وهكذا[2].

(4) الاعتداء على نظام بطاقة الائتمان من قبل موظفي البنك: قد يلجأ موظف البنك إلى استغلال وظيفته وصلاحياته، ويقوم بالاعتداء على بطاقة الائتمان، من خلال تواطئه إما مع العميل نفسه، أو مع التاجر، أو مع الغير وذلك على النحو الآتي:

أ. تواطؤ موظف البنك مع العميل: ويأخذ أكثر من صورة، من خلال استصدار الموظف بطاقة ائتمان للعميل، بمستندات مزورة بالاتفاق بينهما، أو من خلال السماح للعميل بتجاوز السقف الائتماني، من خلال استيلائهم على أموال الغير بدون موافقة البنك، أو من خلال السماح للعميل باستخدام بطاقة منتهية الصلاحية[3].

ب. التواطؤ بين موظف البنك والتاجر، في الاعتداء على البطاقة الائتمانية: ويتمثل ذلك من خلال تجاوز حد السحب، من صرف قيمة إشعارات البيع، مع ضرورة وجود القصد الاحتيالي، أو من خلال الاتفاق، على اعتماد

---

(1) مصطفى، جرائم الحاسبات الآلية في التشريع المصري، ص303.

(2) عبدالرحيم، وجدي عصام، (2011)، سرقة البطاقات الائتمانية من أجهزة الصراف الآلي، متوفر عبر الموقع: www.coeia.edu.sa.

(3) محمد، الحماية الجنائية للتعاملات الإلكترونية، ص162.



موظف البنك إشعارات البيع، استناداً إلى بطاقة مزورة أو منتهية الصلاحية.

جـ- تواطؤ موظف البنك مع الغير : بحيث يتفق موظف البنك مع بعض العصابات المنظمة بتزويدهم بيانات البطاقات الأصلية، لتستخدم بالاستيلاء على المال، مقابل نسبة معينة يتقاضاها موظف البنك، وهكذا أصبح الموظف شريكاً بجريمة منظمة(1).

(5) الاعتداء على نظام بطاقات الائتمان من خلال شبكة الانترنت : إنّ مالك البطاقة، يستخدمها من خلال ذهابه إلى ماكينات الصرف الآلي، أو المتاجر المتعاملة بها بصفته الشخصية، للاستفادة من السلع والخدمات، ولكن ومع تطور امتيازات هذه البطاقة، بات العميل صاحب البطاقة يستطيع أنْ يحصل على السلع والخدمات من دون ذهابه إلى أماكنها، بل من خلال شبكة الانترنت(2)، حيث يقوم بملئ نموذج على صفحة الويب، ويدون بيانات البطاقة والكود الخاص بالسلعة، التي يرغب بشرائها، والعنوان المراد أن ترسل إليه، وهذا ما يسمى بالتجارة الإلكترونية، ومن هنا قد يتعرض أصحاب هذه البطاقات، إلى أعمال احتيالية على بطاقاتهم، بحيث يتم الحصول على هذه البطاقات، بعد التلاعب بأنظمة الاتصال الخاصة بشبكة الانترنت، بوسائل فنية من قبل مختصين، واستخدام أرقام هذه البطاقات المتمثلة بالحصول على السلع والخدمات، ومن أهم أساليب الخداع لهذه الحالة، والمتمثلة من خلال إنشاء مواقع وهمية على شبكة الانترنت على غرار كبرى الشركات المتعاملة في حقل التجارة الإلكترونية، بحيثُ يظهر هذا الموقع الوهمي، مطابق بنسبة كبيرة للموقع الأصلي للشركة، ويقوم بهذه الحالة بتلقي معظم تعاملات الموقع الأصلي، وبعد الإنتهاء من الإستيلاء على الأموال التي تم الحصول عليها، من قبل الضحايا طالبي السلع، يتم إغلاق

---

(1) أبو شامة، عولمة الجريمة الاقتصادية، ص88.

(2) هرول، نبيله، (2007)، الجوانب الإجرائية لجرائم الانترنت، الطبعة الأولى، دار الفكر الجامعي للنشر،الإسكندرية، مصر، ص32.

الموقع بدون معرفة من كان وراء ذلك، من محترفي أساليب الاحتيال الإلكتروني، وغالباً ما يقع مثل ذلك النوع من الجرائم، من خلال عصابات منظمة، مستعينة بذلك بالمختصين في مجال شبكة الانترنت[1].

3.2 كيفية مواجهة جرائم بطاقات الدفع الإلكتروني

نلاحظ أن جرائم بطاقات الدفع الإلكتروني، ما هي إلا انعكاس لواقع الأفعال غير المشروعة، والتي انقسمت بدورها إلى جانبين[2]:

الجانب الأول: أفعال غير مشروعة، كانت محكومة بعلاقات تعاقدية مسبقاً، سواء بين العميل والبنك، أو بين التاجر والبنك، لاعتماد البطاقات.

الجانب الثاني: أفعال غير مشروعة، وهي التي كانت خارج حدود العلاقة التعاقدية، والتي شكلت أيضاً اعتداء على بطاقات الدفع الإلكتروني، مثل الاعتداء من قبل الغير بكافة صوره المتعددة، ومن هنا سنحاول أن نلقي الضوء، على النصوص التشريعية في بعض الدول، في كيفية مواجهة جرائم بطاقات الدفع الإلكتروني، والحلول الفنية المساهمة في الحد منها، من ثم الجهود الدولية في الحد من جرائم الاحتيال الإلكتروني بشكل عام.

1.3.2 المواجهة التشريعية لجرائم بطاقات الدفع الإلكتروني

إن جرائم بطاق ات الدفع الإلكتروني، باتت تشكل تحدياً كبيراً للنظام القانوني، خصوصاً قانون العقوبات، والذي كان في الماضي يجرم الاعتداء على الأشياء المادية المرئية، بعيداً عما يدور من انتهاكات تستوجب التجريم في الثورة المعلوماتية، فإن هنالك الكثير من تشريعات الدول العربية، لم تفرد نصوص تجريميه في الاعتداءات التي تقع على بطاقات الدفع الإلكتروني، إلا القليل من دول الخليج العربي، على عكس الكثير من الدول المتقدمة[3].

---

(1) الرومي، التعاقد الالكتروني عبر الانترنت، ص139 وما بعدها.

(2) القضماني، البطاقة المصرفية والانترنت، ص111.

(3) الملط، الجرائم المعلوماتية، ص150.

وفيما يلي موقف بعض التشريعات على المستوى الدولي والعربي:

نجد أن قانون العقوبات الايطالي، قد جرم أفعال الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، ووضع النصوص الخاصة بذلك، من أجل الحد من ارتكاب هذه الجرائم، وذلك من خلال نص المادة (12)من القانون رقم (72) لسنة 1992التي تنص على أنّه: (يعاقب كل من يسيء استخدام بطاقة ائتمان، أو بطاقة معدنية، أو ما شابها من وسائل السداد إذا ما استخدمها بغرض سلب الأموال، رغم أنّه ليس مالكها الشرعي، أو قام باستعمالها بالسداد النقدي المقدم، أو في سداد قيمة بضائع، أو خدمات بالسجن من عام إلى خمسة أعوام أو الغرامة المالية من (600) ألف إلى 3 ملايين ليرة ايطالية)، إما المشرع الفرنسي فإنّه وضع الحماية الكافية لجرائم بطاقات الدفع الإلكتروني، من خلال القانون رقم (91_1382) الصادر في كانون الثاني لسنة 1991وذلك بإضافة فقرتين إلى نص المادة (67) من قانون العقوبات الفرنسي حيث جاء بالفقر الأولى أنّه: (كل من زيف، أو عدل إحدى بطاقات السداد وكل من استخدم، أو حاول استخدام بطاقة سداد، أو بطاقة معدنية تم تزيفها، أو تعديلها مع علمه بذلك، كذلك كل من اتفق على استلام مستحقات عن طريق بطاقة سداد تم تزيفها، أو تعديلها مع علمه بذلك، يعاقب بالسجن من سنه إلى خمسة سنوات وغرامة مالية تتراوح بين(20,000) فرنك إلى(200,000) فرنك)[1]، إما الفقرة الثانية فقد أوجبت مصادرة البطاقات، أو الأدوات المعدة، أو المستخدمة في التزوير والتقليد إلا إذا استخدمت بدون علم مالكها، مع الإشارة إلى أنّ المشرع الفرنسي، قد جرم الأفعال المرتبطة بنظم المعلومات، وتطبيقات الحاسب الآلي منذ العام 1988[2].

في حين نلمس هذا الحرصَ على الصعيد العربي في التشريع القطري، الذي عالج كل ما يتعلق ببطاقات الدفع الإلكتروني من خلال قانون العقوبات القطري رقم(11) لسنة 2004بعنوان جرائم الحاسب الآلي في المواد (370 لغاية 387)

---

(1) فوزي، وعي المواطن العربي تجاه جرائم الاحتيال"بطاقات الدفع الإلكتروني نموذجاً، ص134، 135.

(2) قورة، جرائم الحاسب الآلي الاقتصادية، ص606.

وجرم العديد من الأفعال غير المشروعة، المصاحبة لاستخدام الحاسب الآلي، وبطاقات الدفع الإلكتروني، حيث نصت المادة (379) على أنّه: (يعاقب بالحبس مدة لا تتجاوز ثلاثة سنوات، كل من استخدم حاسباً آليا، بطريق التلاعب سواء عن طريق إدخال معلومات، أو بيانات زائفة، أو غير حقيقية، أو عن طريق العبث بالبرامج) وهذه المادة ، يمكن أن تطبق على كافة أفعال التصيد الاحتيالي لأرقام وبيانات بطاقات الدفع الإلكتروني، ونصت المادة (381) من القانون ذاته على أنّه : (يعاقب بالحبس مدة لا تتجاوز خمس سنوات، كل من استولى بغير حق على أموال البنوك، أو العملاء لديها عن طريق استخدام بطاقات الدفع الإلكتروني الممغنطة، التي يصدرها البنك سواء أكانت خاصة به، أو بعميل آخر)، ونرى كيف أن المشرع القطري، تناول بطاقات الدفع الإلكتروني بشكل مباشر، في محاولة منه لسد أيّ ثغرة تشريعه من الممكن التحايل، أو الاحتجاج بها قانوناً، ولم يكتف بذلك، بل وضع بعض التفصيل لكيفية تجريم الاعتداء على هذه البطاقات، وذلك من خلال نص المادة (382) التي تنص على أنّه: (يعاقب مدة لا تقل عن ستة أشهر ولا تتجاوز ثلاثة سنوات، وبالغرامة التي لا تقل عن عشرة آلاف ريال ولا تزيد عن عشرين ألف ريال كل من[1]:

أ. كل من حاز، أو استخدم آلات صنع بطاقات الدفع الآلي، دون تصريح من الجهات المختصة.

ب. كل من حاز، أو أحرز بطاقة دفع آلي مزورة، أو مسروقة مع علمه بذلك.

ج. كل من حاز، أو أحرز بطاقات دفع آلي، معدة للإصدار دون تصريح بذلك من البنك.

د. كل من حاز بغير تصريح من البنك، آلات ومعدات طباعة بطاقات الدفع الإلكتروني.

ه. كل من حاز أدوات يدوية أو آلية، مما يستخدم في إتمام التعامل ببطاقات الدفع الإلكتروني دون تصريح.

---

(1) راجع النص الكامل لقانون العقوبات القطري رقم 11 لعام 2004 على الرابط الآتي:
www.gcc_legal.org/mojportalpublic/BrowseLawOption.aspx?country=3&LawID=2597



2.3.2 الحلول الفنية المساهمة في مواجهة جرائم بطاقات الدفع الإلكتروني

نظراً لزيادة الاستخدام غير المشروع لجرائم بطاقات الدفع الإلكتروني، سواء من قبل حاملها، أو من قبل الغير، وما يترتب عليها من خسائر مالية، تهدد جميع أطراف العملية التجارية، لكل من حامل البطاقة والتاجر والبنك، فإنّ مواجهة مثل هذا النوع من الجرائم، توجب التعاون من كل الجهات، بحكم أن الإجراءات التشريعية قد تكون غير كافية، في وضع آلية معينة للحد من ارتكاب هذه الجرائم، سواء من خلال أجهزتها الأمنية والقضائية، فما كان من المؤسسات المالية الدولية مثل مؤسسة فيزا، ومؤسسة ماستركارد، إلا أنْ تطرح العديد من الحلول الفنية، ووضع بعض المعايير، التي تساعد في وضع حد لهذه الجرائم والفصل في النزاعات التي قد تنشئ، بين أطراف العملية التجارية سيما البنوك [1]، كما اتخذت البنوك النهج ذاته في تطوير أنظمتها المصرفية، وتأمين شبكات المعلومات الخاصة بها، وتقديم كافة سبل الدعم والحماية لعملائها من التجار وحاملي البطاقات، من الوقوع في شرك هذه الجرائم الاحتيالية، خصوصاً أن البًنوك، وهذه المؤسسات المالية تعد هي المتضرر الرئيسي من هذه العمليات الاحتيالية؛ لأنها ذات مساس بسمعة وثقة العملاء بها، والعمل من خلال التعاون مع أكبر عدد من المصرفيين المختصين، مثل مؤتمر قمة العلاقات الحكومية المنعقد في الفترة من 16 إلى 18 في فندق النهضة في العاصمة واشنطن والذي استدعاء (800) شخص من المصرفين أصحاب الخبرة، في التعاملات المصرفية؛ وذلك من أجل التباحث لمواجهة هذه الأخطار، ووضع الخطط اللازمة لمواجهتها في بادرة منها لإثبات مدى اهتمام القطاع المصرفي، بتوفير مناخ مالي سليم قدر المستطاع، من خلال التصدي لهذا النوع من الجرائم [2].

---

(1) الجهني، أمجد حمدان، (2010)، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، الطبعة الأولى، دار المسيرة للنشر، عمان، الأردن.

(2) Johnson, A., (2010) , Stand up for banking at ABA,s GR Summit. ABA banking journal. Vol. 2.



(1) الحلول الفنية في نطاق المؤسسات المالية:

إنّ مؤسسة فيزا وماستركارد، واللتان تعدان من كبريات المؤسسات المالية، المصدرة لبطاقات الدفع الإلكتروني، وحرصاً منهما قامتا بتطوير أنظمتهما وذلك من خلال تأمين العمليات التي يتم إجرائها عبر شبكة الانترنت، باستخدام بطاقات الدفع الإلكتروني، ومن شأن هذا النظام أن يعرف التاجر بصاحب البطاقة، في حال التعامل بها عبر الشبكة والعكس مع تشفير هذه البيانات المستخدمة أثناء التعامل؛ بغية حمايتها من العمليات الاحتيالية، في محاولة لإثبات مدى اهتمام هذه المؤسسات المالية، في الحدّ من ظاهرة جرائم الاحتيال الإلكتروني(1).

(2) التحول إلى البطاقات الذكية (Smart Card):

تسعى المؤسسات المالية في الإطار ذاته إلى حث وتشجيع البنوك في مختلف دول العالم، إلى التحول لما يسمى بالبطاقات الذكية، كبديل عن البطاقات الممغنطة، ومن المتوقع أن يؤدي انتشار مثل هذه البطاقات، إلى الحدّ من جرائم بطاقات الدفع الإلكتروني، وإنْ كانت تصطدم ببعض العقبات، مثل التكلفة المادية العالية لهذه البطاقات، من خلال إعادة تجهيز مراكز الإصدار، واستبدال وحدات نقاط البيع الممغنطة الموجودة لدى التجار، ومكاتب الخدمات من أجل ت فعيل نطاق العمل بالبطاقات الذكية، والبطاقات الممغنطة على حداً سواء، ونجد الأمر ذاته

---

(1) فوزي، وعي المواطن العربي تجاه جرائم الاحتيال"بطاقات الدفع الإلكتروني نموذجاً، ص157. تجدر الإشارة إلى أن أهم الحالات التي ينص عليها عقد حامل البطاقة كسبب لإلغاء البطاقة:

(أ) في حالة عجز، أو توقف الحامل عن الدفع.

(ب) في حالة إشهار إفلاس الحامل، أو الكفيل بحكم قضائي.

(ج) في حالة الحجز على ممتلكات حامل البطاقة، أو الكفيل.

(د) في حالة وفاة الحامل، أو الكفيل.

(ه) في حالة طلب الحامل إلغاء البطاقة.

(و) في حالة إخلال الحامل بالشروط والالتزامات الواردة في العقد. لمزيد من التفاصيل انظر الجهني، المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني، ص140.

لماكينات الصرف الآلي، ويأتي ذلك من خلال ابتكار مؤسسة فيزا الدولية، بطاقات ذكية متطورة من خلال احتوائها على ذاكرة الكترونية، ومعالج صغير يدعى Micro (Processor) حيث تتمكن هذه البطاقة، من إنتاج أرقام سرية مختلفة بعد كل عملية شراء تم استخدام البطاقة من خلالها، وذلك بمجرد الضغط بالإصبع على المعالج، من أجل تأمين عمليات التعامل بالبطاقة، سواء أكانت عمليات مباشرة مع التاجر، أو من خلال استخدام الهاتف، أو من خلال البريد الإلكتروني عبر شبكة الانترنت [(1)]، مع العلم أنه تم طرح هذه البطاقات بالأسواق

(3) الحلول الفنية في نطاق البنوك

اتجهت العديد من البنوك، خاصة في الدول المتقدمة، إلى تطبيق نظام الشبكة العصبية (Nedronet)، وهو برنامج من برامج الحاسب الآلي المتطورة، والذي يعمل على مراقبة كافة التعا ملات المصرفية، التي تتم بواسطة البطاقات الخاصة بالبنك، واكتشاف العمليات المشبوهة إلكترونياً، حيث يعتبر من البرامج الرائدة في هذا المجال[(2)].

كما اتجهت بعض البنوك، إلى تطبيق نظام يعتمد على استخدام خدمة الرسائل القصيرة (SMS) المستخدمة بالهواتف النقالة، من أجل تنبيه وإعلام عملائها

---

(1) القضماني، البطاقة المصرفية والإنترنت، ص26 وما بعدها. تجدر الإشارة إلى وجوب التفرقة بين مصطلح النقود الإلكترونية، ومصطلح الدفع الإلكتروني فمصطلح الدفع الإلكتروني: مصطلح واسع حيث يتضمن جميع الوسائل التي تستخدم في تكنولوجيا المعلومات من أجل الوفاء، ومثالها الشيكات الإلكترونية، ونظام التحويل الإلكتروني للأموال، والكمبيالة الإلكترونية، أي الدفع بالكروت البنكية سواء أكانت ائتمانية، أو خصم، أما النقود الإلكترونية: فأنها إحدى وسائل الدفع الإلكتروني، وتمتاز بأن هذه الوحدات الإلكترونية المستخدمة بالوفاء تعمل على أداة مستقلة عن الحساب الموجود بالبنك، بحيث يتم الصرف من خلال هذه الأداة بعيداً عن الحساب الخاص بالعميل، وقد تكون هذه الأداة عبارة عن برنامج يتم تحميله على ذاكرة الحاسب الآلي الخاص بالعميل. لمزيد من التفاصيل أنظر غنام، محفظة النقود الإلكترونية رؤية مستقبلية، ص7 وما بعدها.

(2) فوزي، وعي المواطن العربي تجاه جرائم الاحتيال"بطاقات الدفع الإلكتروني نموذجاً، ص106.

وبشكل فوري، لكل عملية يتم فيها استخدام البطاقة، سواء من خلال السحب النقدي من أجهزة الصرف الآلي، أو من خلال عمليات الشراء من المتاجر، أو عبر شبكة الانترنت، وبمجرد وصول الرسالة للعميل، فإنّه يكون على علم بوقت استخدام البطاقة، وحجم المبلغ المستهلك، وهذا يحد من خطر أي عمل احتيالي، قد ينال من البطاقة المصرفية للعميل [1]، خصوصاً أن هذه العملية تتم بصورة آلية، وعلى مدار الساعة، في حين قامت بعض البنوك، بمنح عملائها بطاقات خاصة للتعامل بها عبر عمليات الشراء من خلال شبكة الانترنت، ذات سقف ائتمان محدد، مع إمكانية زيادة هذا السقف بطلب العميل، من خلال بعض ضوابط الآمان المفروضة لهذه البطاقة من البنك، وذلك من أجل التقليل من حجم الخسائر، التي يتعرض لها عملائها، من خلال عمليات الشراء عبر شبكة الانترنت، والتي تتسبب بخسائرَ مالية كبيرة نتيجة هوس البعض في ممارسة أعمال الشراء عبر الانترنت، خصوصاً لبعض السلع التي تكون غير متوفرة بشكل أو بآخر، أو محتكرة لدى كبرى الشركات، فما من سبيل إليها إلا السفر، أو شرائها عبر الانترنت[2].

وقد قامت بعض البنوك، في محاولة منها أيضاً، للحد من الجرائم الواقعة على بطاقات الدفع الإلكتروني، بإصدار بطاقة تحمل صورة العميل مالك البطاقة، على غرار البطاقة الشخصية، خصوصاً للبطاقات الذهبية ذات السقف الائتماني

---

(1) عبد الحليم، عماد الدين، (2010)، المعاملات المصرفية بواسطة الهواتف النقالة، رسالة ماجستير غير منشورة، كلية الحقوق، جامعة الشرق الأوسط، عمان، الأردن، ص26.
كشفت وحدة الجرائم الالكترونية البريطانية (CCU) Cyber Crime Unit عن محاولة احتيال عبر الانترنت، تتمثل بقيام محتالين بإنشاء تأمينات بنكية مزيفة داخل أوروبا في أكثر من (29) موقع انترنت، بحيث تظهر ملفات مزيفة وكأنها تدار من قبل بنوك أوروبية نظيفة، وقد لوحظ أن مئات الآلاف من الدولارات دفعت لهذه التأمينات الاحتيالية، وإن هذه المواقع الاحتيالية استقبلت أكثر من (400) مليون دولار، وأن إجمالي الملفات المزيفة تقدر بحوالي (309) بليون دولار أمريكي. لمزيد من المعلومات حول هذه العملية أنظر الموقع الالكتروني الآتي:
http://search.conduit.com/ResultsExt.aspx?ctid=CT2845289&SearchSource=2&q=www.icc+wbo.org%2Fccs%2FNews_archives%2F2001%2Ffraud.Asp
(2) غنام، محفظة النقود الإلكترونية رؤية مستقبلية،، ص16.

العالي، وبهذه الحالة لا يستطيع أي شخص استخدام هذه البطاقات من خلال عمليات الشراء من المتاجر (نقاط البيع) على أقل تقدير، حيث قام الـ بنك العربي الأردني ومنذ العام 2000، بإصدار مثل هذه البطاقات، ومن هنا يجب أن لا يفوتنا ضرورة، الاهتمام بموظفي البنوك المسؤولين في مراكز البطاقات، وآلية تدريب هؤلاء الموظفين وتوعيتهم إلى حجم الأخطار المرافقة للسلوك المالي المشبوه، وكيفية التعامل مع العملاء و التجار، والذين في الغالب ما نجدهم يطالبون بالسرعة والتميز، في تقديم الخدمة لهم [1]، بحكم تعدد وكثر البنوك، والتنافس في تقديم الخدمات، فيما بينها إما التجار فإنّه يتوجب عليهم أيضاً، المساهمة بمكافحة انتشار وتفاقم العمليات الاحتيالية، الواقعة على بطاقات الدفع الإلكتروني؛ لكي لا يقع التاجر أيضاً ضحية أحد الأساليب الاحتيالية، وكونه أحد أطراف العملية التجارية الرئيسية لبطاقات الدفع الإلكتروني، فإنّه يتوجب عليه مايلي:

(1) التأكد من شخصية مستخدم البطاقة، وأنّه هو الحامل الشرعي لها.

(2) التأكد من توقيع صاحب البطاقة، وأنّه لم يتعرض للمحو.

(3) عدم قبول واعتماد أي بطاقة، عندما تكون مقدمة من قبل شخص آخر، غير صاحبها الأصلي.

وبهذه الحالة تصبح الحلول الفنية، ذات فعالية أكثر عندما نجد دراية وتعاون، من قبل التاجر الذي يعتبر أكثر الأطراف احتكاك بحامل البطاقة[2].

أما صاحب البطاقة، فيتوجب عليه هو الأخير، أن يساهمَ مع باقي الأطراف التجارية وبحد أدنى، ألاّ يجعل من نفسه فريسة، لإحدى جرائم بطاقات الدفع

---

(1) الشورة، جلال عايد، (2008)، وسائل الدفع الإلكتروني، الطبعة الأولى، دار الثقافة للنشر، عمان، الأردن، ص105. تجدر الإشارة وبحسب معلومات صادرة عن منظمة (CSC) والمختصة بمجال تكنولوجيا المعلومات، أنّه يوجد بالعالم أكثر من (25) مليون من نقاط البيع، التي تعتمد الدفع بالبطاقة المصرفية حتى العام 2002. لمزيد من التفاصيل أنظر القضماني، البطاقة المصرفية والانترنت، ص27.

(2) فوزي، وعي المواطن العربي تجاه جرائم الاحتيال"بطاقات الدفع الإلكتروني نموذجاً، ص160، 161.

الإلكتروني، وفيما يلي بعض المحاذير والنصائح، التي يجب على حامل البطاقة الأخذ بها:

(1) حفظ الرقم السري في الذاكرة فور الحصول عليه، وعدم اطلاع أيّ أحدٍ عليه، وفي حال اضطر الحامل إلى كتابته، فيجب عدم حفظة في نفس المكان الذي يحتفظ به بالبطاقة[1].

(2) عند اختيار وتغيير الرقم السري، يتوجب على حامل البطاقة الابتعاد عن الحروف، والأرقام ذات الدلالة على شخص المستخدم، مثل رقم الهاتف، أو تاريخ الميلاد وهكذا.

(3) فحص فاتورة الشراء، والتأكد منها قبل التوقيع عليها.

(4) التأكد من استرداد البطاقة، بعد عملية الاستخدام قبل مغادرة المكان الذي تمت به العملية.

(5) عدم التوقيع على فواتير وإشعارات فارغة، من بيانات الشراء لكي لا يتم تعبئتها من قبل التاجر، والمطالبة بقيمتها من قبل البنك[2].

ومن جهة نظر الباحث، إنّ حامل البطاقة يقع على عاتقة الجزء الأكبر من المسؤولية، من خلال التزامه بمثل هذه المحاذير والنصائح، التي تؤدي وبشكل حقيقي، إلى الحدّ من انتشار جرائم بطاقات الدفع الإلكتروني، خصوصاً أننّا كثيراً ما نسمع أن النصيب الأكبر من العمليات الاحتيالية تقع على حامل البطاقة بشكل أقل من التجار، والذين غالباً ما يتمتّعون بالحيطة والحذر أكثر من غيرهم، ومع ذلك - للأسف- نادراً ما نجد مثل هذه المحاذير والنصائح، تنشر بصورة أكثر شمولية، لتصل إلى أكبر عدد ممكن من الأشخاص مستخدمي البطاقات، فلا نجدها إلا في المؤلفات وعند أصحاب الاختصاص، والذين من النادر أن نرى أي نشاط توعوي من خلالهم، خصوصاً مع ضعف وسائل الإعلام لدينا، في تسليط الضوء على مثل هذه الموضوعات، بشكل يساهم في الحدّ من انتشار جرائم البطاقات، وفيما يتعلق بماكينات الصرف الآلي، سنحاول أن نبين الآلية الآمنة باستخدام هذه الماكينات

---

(1) الشورة، وسائل الدفع الإلكتروني، ص70.

(2) الشناوي، جرائم النصب المستحدثة، ص135 وما بعدها.

خصوصاً بعد الانتشار غير المسبوق لهذه الخدمة واعتماد عدد كبير من المستخدمين لهذه البطاقات عليها؛ لما توفره من جهد وسهولة في تبادل الأموال على مدار الساعة بلا انقطاع، فما كان من المحتالين، إلا أن يضعوا هؤلاء المستخدمين لهذه الخدمة نصب أعينهم، ولذلك نذكر أهم النصائح الإرشادية والتحذيرية، للاستخدام الآمن لماكينات الصرف الآلي على النحو الآتي:

1. أخذ الحيطة والحذر من البيئة المحيطة لماكينات الصرف الآلي، بالابتعاد عنها، في حال دارة الشكوك حول أشخاص بهذا المحيط.
2عدم التوجه إلى ماكينات الصرف الآلي، في أوقات متأخرة من الليل، وإذا دعت الضرورة يتوجب، أن يكون برفقة المستخدم بعض المعارف الموثوقين لتجنب مخاطر النهب والسرقة[1].

3.3.2 الجهود الدولية في مكافحة جرائم الاحتيال الإلكتروني

رأينا كيف ساهم التطور الملحوظ، بنظم تكنولوجيا المعلومات، إلى استحداث العديد من جرائم الاحتيال الإلكتروني، وإيقاع الآلاف من ضحاياه على المستوى العالمي، فما كان من الدول والمنظمات ذات العلاقة، إلا أن تفرز بدورها حماية أكثر شمولية وتعاونية، على المستوى الدولي، وذلك من خلال الاتفاقيات الدولية، وعقد المؤتمرات، سواء على صعيد المؤسسات المالية ذات الاختصاص، أو على صعيد الدول، والعمل أيضاً على صياغة نماذج قانونية مشتركة بين هذه الدول، في محاولة منها لتوحيد الجهود، وآليات الحد من الجرائم على الصعيد الدولي، بدل من العمل بشكل منفرد وتعارض سبل المكافحة، سيما فيما يتعلق في التعاون لقبض وتسليم المجرمين، كون مثل هذا النوع من الجرائم، بات يُحتّم تضافر الجهود الدولية مع بعضها البعض، لكونها من الجرائم العابرة للحدود، ولا تعيقها الأبعاد الجغرافية[2].

ومن أهم هذه الجهود على المستوى الدولي مايلي:

---

(1) سفر، أنظمة الدفع الإلكتروني، ص158 وما بعدها.

(2) أحمد، أمن الانترنت المخاطر والتحديات، ص128.



(1) معاهدة بودابست بخصوص جرائم الحاسبات المعلوماتية والاتصال:

وُقعّتْ هذه المعاهدة بتاريخ 2001/11/23 في العاصمة المجرية بودابست، والتي حملت اسم هذه المعاهدة، حيث وَقعّتْ 26 دولة في نطاق هذه المعاهدة، في حين كانت كل من كندا، واليابان، وجنوب إفريقيا، والولايات المتحدة الأميركية، أول من وقع معاهدة دولية، بشأن الأفعال الإجرامية المتعلقة بالحاسب الآلي، ونظم الاتصالات واستخداماتها، بحيث تناولت هذه المعاهدة، (48) مادة موزعة على أربعة فصول، تضمنت عدد من التعريفات الخاصة بهذا النوع من الجرائم، وكيفية سبل التعاون الأمني والقضائي، وتبادل المعلومات، وتسليم الجناة فيما بينها، حيث خُصص الفصل الأول من هذه المعاهدة فقط، من أجل التعريف ببعض المصطلحات الفنية، الخاصة بتكنولوجيا المعلومات؛ بغية توحيد المفاهيم بين الدول، قبل رسم السياسة العامة لهذه المعاهدة[1].

(2) المنظمة الدولية للشرطة الدولية الانتربول (Interpol):

الانتربول: يعد أكبر منظمة شرَطية دولية، حيث تأسست في العام (1923)، من أجل تفعيل التعاون الشرُطي الَجنائي على الصعيد الدولي، وتظم بعضويتها (186) دولة من الأعضاء، بحيث تدعم هذه المنظمة، جميع المنظمات، والسلطات، والأجهزة الأمنية، التي تساهم في الحدّ من الإجرام البشري الدولي ومكافحته، ومن ضمنها جرائم الاحتيال الإلكتروني، وفي العام 1999 قامت المنظمة بتوقيع اتفاق دوليّ، بين عدد من المنظمات والمؤسسات المالية الدولية المسؤولة عن إنتاج وتوزيع بطاقات الدفع الإلكتروني[2].

ولم تقف منظمة الانتربول عند هذا الحدّ، بل سّارعت إلى تبني مشروع يدعى جولدفيش (Phish Gold)، بعد انتشار ظاهرة الاحتيال الإلكتروني، عبر شبكة الانترنت، حيث هدف هذا المشروع، إلى تكثيف الجهود الدولية، وذلك من العام

---

(1) فوزي، وعي المواطن العربي تجاه جرائم الاحتيال"بطاقات الدفع الإلكتروني نموذجاً، ص150.

(2) محمد، مصطفى، (2011)، دور الانتربول الدولي بمكافحة الجريمة، متوفر عبر الموقع: .www.qanon302.net/news/news.php?action=view&id=5998



2005، حيث وصل عدد الدول المشاركة في المشروع، إلى 24 دولة، وفيما يلي بعض الأهداف التي تبناها المشروع ونذكر منها:

(أ) التنسيق في إجراء التحريات على المستوى الدولي لمواجهة هذا النشاط.

(ب) إعداد شبكة خاصة بطرق البحث المتخصصة بكل دولة من الدول.

(ج) متابعة أثر جميع الأموال، ومتحصلات هذا النشاط الإجرامي دولياً.

(د) اتخاذ الإجراءات الوقائية على المستوى المحلي والدولي لمنع مثل هذه الجرائم[1].

(3) التحالف العالمي لمكافحة التصيد الاحتيالي على شبكة الانترنت:

وجاء هذا التحالف نتيجة التزايد الملحوظ لعمليات الاحتيال الإلكتروني عبر شبكة الانترنت، والاستيلاء على بطاقات الائتمان، وأرقامها بطرق احتيالية، تؤدي في نهاية الأمر إلى إلحا ق خسائر في الأموال، وحقوق مستخدمي الانترنت، وهذا بدوره انعكس سلباً على مواقع التجارة الإلكترونية المشهورة على الانترنت، الأمر الذي دفع المسؤولين والقائمين على إدارة هذه المواقع، إلى تشكيل تحالف، ضم أكثر من 1600 من الشركات التجارية والمؤسسات المالية، والمنظ مات المسؤولة عن بطاقات الدفع الإلكتروني، مثل فيزا وماستركارد، وعدد كبير من البنوك وشركات تكنولوجيا المعلومات، وذلك من خلال جمع المعلومات الفنية حول المواقع، والمصادر المتورطة بعمليات احتيالية، ووضعها في قاعدة بيانات تدعى (شبكة تقارير الاحتيال) التي تقوم بـ نشرها الكترونياً على شبكة الانترنت، وفي المجلات ذات الاختصاص، لتبيح لجميع مستخدمين الانترنت، الاطلاع على هذه المواقع؛ لتجنب التعامل معها، وما كان من شركة مايكروسوفت، إلا أن طورت برنامج يدعى (انترنت اكسبلورر 7) الذي يُمكّنُ الّمستخدم من اكتشاف الرسائل الخادعة، والمواقع الاحتيالية، أثناء التصفح على الشبكة، هذا ونجد أيضاً أن المؤتمرات، تشكل فرصة كبيرة ومميزة، لتبادل الخبرات بين الدول المشاركة ووضع الآلية

---

(1) فوزي، وعي المواطن العربي تجاه جرائم الاحتيال"بطاقات الدفع الإلكتروني نموذجاً، ص153. لمزيد من التفاصيل أنظر الموقع الرسمي لمنظمة الانتربول على الرابط الآتي: www.interpol.org

المناسبة، لمكافحة هذا النوع من الجرائم، من خلال التعرف على كل ما تم الوصول إليه، من آليات، وبرامج الحماية الـ متعلقة بأمن المعلومات بشكل عـام، والاحتيـال الإلكتروني بشكل خاص [1]، لذلك بات الكثير من المؤتمرات، تُعقـد بـشكل دوري ومنتظم، على المستوى الدولي، وحتى على مستوى الدولة الواحدة، من خلال بعض المؤسسات والشركات العاملة، على المستوى الداخلي أكثر منه على الصعيد الدولي، فنجد أن قسم الأخطار، بمنظمتي فيزا وماستركارد العالمية يتولى عقـد مـؤتمرات سنوية، يشارك فيها المختصون من أجهزة المكافحة من الدول المـشاركة، وكـذلك مسؤولي الأخطار بمراكز البطاقات بالمؤسسات المالية، بهدف الحد من انتشار هذه الجرائم، وكان للمؤتمرات أثر واضح منذ ع قود، حيث بدأ التعاون الدولي، من خلال مؤتمر الأمم المتحدة السابع، الذي عقد عام 1995 الخاص بمنع الجريمة، والمؤتمر الثالث لمنع الجريمة بفنزويلا، عام 1990 والمؤتمر الوزاري العالمي في نـابولي بإيطاليا، عام 1994الذي أعطى الأولوية للجريمة المنظمة في بادرة منهـا لتأكيـد مدى اهتمام، ومقدرة هذه المؤسسات، على الوقوف جنباً لجنب مع المجتمع الدولي، في وضع السياسات والحلول، المساهمة في الحد مـن انتـشار جـرائم الاحتيـال الإلكتروني [2]، ومن المؤتمرات على الصعيد العربي المـؤتمر الـسادس للجمعيـة

---

(1) التحالف العالمي لمكافحة التصيد الاحتيالي متوفر عبر الرابط: www.antiphishing.org

(2) المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية، ص419 وما بعدها. تجدر الإشارة أن هونج كونج تمتاز بأفضل شبكة اتصالات الكترونية في قارة أسيا، حيث نجد أن هنالك أكثر من 130 شركة من الشركات التي تقدم خدمة الانترنت موجودة فيها، بالإضافة إلى ابتكار هونج كونج في العام 1996 أحد أكثر وسائل التقدم التكنولوجي على المستوى العالمي، لإجراء عملية الدفع الإلكتروني، والمقاصة للمبالغ الكبيرة (RTGS)، وأن هذا التطور قد ساعد المستخدمين المحليين والدوليين في الحصول على كل ما تفرزه الأسواق العالمية في مجال تكنولوجيا المعلومات وغيره بكل سهوله وأمان، وأن اللجنة المسؤولة عن البنية التحتية لهونج كونج أبرزت تقدما واضحاً وملحوظ، من خلال إعدادها لأنظمة المخاطر في العمليات المالية. الشورة، وسائل الدفع الإلكتروني، ص122 وما بعدها.

المصرية للقانون الجنائي عام 1993، والذي تناول جرائم الحاسب الآلي والجـرائم الأخرى في مجال تكنولوجيا المعلومات، حيث يُعتبـر هـذا المـؤتمر تحـضيرياً، للمؤتمر الدولي الخامس عشر، للجمعية الدولية لقانون العقوبات، الذي عقد بالبرازيل عام 1994، والذي وضع توصيات حول جرائم الحاسب الآلي، والانترنت، وكيفيـة التحقيق فيها وضرورة إدخال التعديلات اللازمة في القوانين الجنائية، مـن أجـل مواكبة مستجدات هذه الجرائم، مع الإشارة إلى أن دولة السويد، تُعد الأولى علـى المستوى العالمي، التي قامت بسن تشريعات ذات علاقة، بجرائم الحاسـب الآلـي والانترنت، وذلك من خلال قانون البيانات السو يدي، لعام 1973 والذي عالج قضايا الاحتيال الإلكتروني عن طريق الحاسب الآلي، وهذا يدفعنا إلى الإقرار، أنّ غالبيـة الدول المتقدمة، قد كانت على قدر كافي من الجدية في التعـاطي مـع المخـاطر المتمخضة عن الثورة المعلوماتية، في محاولة منها، لإرساء أكبر قدر ممكن مـن الأمان الإلكتروني من خلال سن التشريعات اللازمة لذلك[1].

ومن جهة نظر الباحث، أن العائق الحقيقي الذي يعرقل مسيرة التطور، في مجال الحماية الإلكترونية بإطارها العام، على صعيد الدول العربيـة، ودول العـالم الثالث، لا يكمن في قلة عقد المؤتمرات المحلية، والدوليـة، ووضـع ا لتوصـيات، والبروتوكولات، وإنّما من خلال عدم تطبيق ما تتمخض عنه هذه الجهود بـصورة فعلية على أرض الواقع، والاكتفاء بتدوينها على الورق، ومن المعوقات أيضاً، قلـة

وهنالك نوع من الاحتيال الإلكتروني، يسمى الاحتيال الإلكتروني على الجامعات، من خلال قيام بعض الطلبة المحترفون من اختراق أنظمة الحاسب الآلي الخاصة بالجامعة، والعمل على التحايل على هذه الجامعة من خلال تغيير الدرجات والمعدلات والتلاعب بهذه النتائج إلكترونياً، واستخدام الماسحات الضوئية بصورة احتيالية؛ بغية الحصول على المنح الدراسية، أو تكاليفها المالية، ولم نتطرق لهذا الموضوع بشي من التفصيل وذلك لعدم انتشار مثل هذا النوع من الاحتيال الإلكتروني في البلدان العربية، مقارنة مع الدول الغربية وخصوصاً الولايات المتحدة الأمريكية، ومع ذلك كان من الضرورة بمكان ضرورة الإشارة إليه أنظر ذلك من خلال: Sauter, D., (1998) , Electronic fraud on campus. The electronic campus. Vol6.

(1) أحمد، أمن الانترنت المخاطر والتحديات، ص129 .

الانفراد بجهات أكاديمية متخصصة، لرسم سياسات فاعلة من أجل مكافحة مثل هذا النوع من الجرائم، وإلقاء جُل هذه الأفعال في الغالب، على عاتق الأجهزة الأمنيـــة، والتي بدورها لن تستطيع من السيطرة على الأمور بمفردها، وهذا يدلنا على ضعف التعاون بين الأجهزة، والدوائر ذات العلاقة فيما بينها، وأن كانت مثل هذه الآليـــات وسبل الحماية، تختلف من حيث قصورها ونجاعتها من دولة إلى أخرى، وأنّـــه لا سبيل لحل هذه الأزمة، إلا العمل الجدي داخل إطار الدولة الواحدة، من ثم الشروع بالتعاون على الصعيد الدولي.

وإذا نظرنا إلى الواقع الإحصائي، في السنوات الأخيرة للجرائم الإلكترونيـــة في الأردن، وما تمخض عنها من جرائم احتيال الكتروني، نجد أن في العام 2008، بلغ عدد مستخدمي الانترنت في العالم، ما يزيد عن المليار ونصف المليار، أي مـــا نسبة (25%) من مجموع السكان، أما في الأردن فقـــد بلغـــت نـــسبة مـــستخدمي الانترنت، في العام 2000، حوالي (126,000) مستخدم، ما نسبته (2,45%) مـــن إجمالي سكان المملكة، في حين ارتفع العدد في العام 2009، ليصبح (1,126,700) من إجمالي عدد سكان المملكة، أي ما نسبته (26%) مـــن عـــدد الـــسكان، وفـــي إحصائية قام بها قسم الإسناد والتحقيق الفني، فرع جرائم تكنولوجيا المعلومات فـــي إدارة البحث الجنائي، الأردن في الفترة من 1 كانون الثـــاني 2009، ولغايـــة 30 تشرين الثاني 2009، والتي تبين عدد الجرائم ذات الصلة، التي تعامل معها القـــسم وغالبية هذه الجرائم انتهت بالإدانة:

نوع الجريمة: انتحال شخصية بلغت 43 جريمة.

تهديد الكتروني بلغت 25.

تشهير وابتزاز الكتروني بلغت 73 جريمة.

قرصنة واحتيال على أجهزة الصرف الآلي بلغت 20 جريمة.

سرقة بريد الكتروني بلغت 25 جريمة.

إنشاء موقع وهمي بلغت 2 جريمة.

سرقة بيانات الكترونية بلغت 15 جريمة.

سرقة بنك الكترونياً بلغت 4 جرائم.



سرقة مواقع الكترونية بلغت 2 جريمة.

جرائم الإساءة للأطفال جنسياً بلغ 1 جريمة، تقارير خبرة فنية بلغت 4 بمجموع وصل إلى 237 جريمة خلال هذه الفترة فقط، مع الإشارة إلى أن مجموع قضايا جرائم الاتصالات، بلغت لوحدها خلال هذه الفترة 2998 قضية تم التعامل معها من خلال هذا القسم(1).

4.2 المواجهة التشريعية لجرائم الاحتيال الإلكتروني في التشريع الأردني

أن جرائم الاحتيال الإلكترو ني أصبحت واقعاً يطال المجتمعات ككل والمجتمع الأردني بشكل بات من الضرورة وجود نصوص تشريعية للحدّ من هذه الجرائم.

سوف نقسم ال قسم إلى ثلاثة أجزاء نتناول بال جزء الأول، المواجهة التشريعية لجرائم الاحتيال الإلكتروني في قانون العقوبات، وال جزء الثاني، نتناول به مدى مواجهة قانون المعاملات الإلكترونية، وقانون جرائم أنظمة المعلومات لجرائم الاحتيال الإلكتروني، وال جزء الثالث، نتناول به دور الأجهزة الأمنية والجهات المتخصصة، في الحد من جرائم الاحتيال الإلكتروني في الأردن.

1.4.2 المواجهة التشريعية لجرائم الاحتيال الإلكتروني في قانون العقوبات

يعتبر الاحتيال الإلكتروني من الجرائم المستحدثة، التي يزداد معدل ارتكابها يوم بعد يوم، وذات تطور مستمر وملحوظ، كونها مبنية على الاستخدام غير المشروع لتكنولوجيا المعلومات، حيث أن قانون العقوبات الأردني، قد خلى من أي نص صريح، لتجريم مثل هذه الجرائم المستحدثة، واكتفى بالتصدي لجرائم الاحتيال بمفهومها التقليدي(2).

---

(1)إدارة البحث الجنائي، قسم جرائم تكنولوجيا المعلومات والإسناد الفني، مديرية الأمن العام، الأردن.

(2) المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية، ص141.

ولكن يُثار التساؤل، عن مدى انطباق النصوص الناظمة، لجريمة الاحتيال التقليدية، في قانون العقوبات الأردني، على جرائم الاحتيال الإلكتروني، من أجل تفادي هذا النقص التشريعي، والحدّ منانتشار مثل هذه الجرائم المرافقة لتكنولوجيا المعلومات.

أولاً: مدى إمكانية الاحتيال على جهاز الحاسب الآلي والنظام المعلوماتي المرتبط به

كما أسلفنا بالتعريف بجريمة الاحتيال التقليدية، التي نظمها المشرّع الأردني، في قانون العقوبات، في المادة (417) التي تنص على أنّه: (كل من حمّل الغير مالاً منقولاً، أو غير منقول، أو إسناداً تضمن تعهداً، أو إبراءاً فاستولى عليها احتيالاً...)، وذكر بعدها الأفعال المجرمة، وحدد العقوبة بالحبس من ثلاثة أشهر إلى ثلاثة سنوات، من غير ذكر تعريف محدد لجريمة الاحتيال، مثل غيره من التشريعات العربية، وعلية فإنّ الاتصال في جريمة الاحتيال التقليدية، ينصب بين الجاني، وشخص آخر يمارس الجاني نشاطه الاحتيالي عليه [1]، على خلاف الاتصال الذي في جريمة الاحتيال الإلكتروني، الذي يتم بين الجاني، وأجهزة الحاسب الآلي، والأنظمة الإلكترونية، كما هو الحال في التحويل الإلكتروني للأموال، بدون وجود التدخل البشري المباشر فيه، وقد أثار ذلك جدلاً فقهياً، حيال مسألة الاحتيال على أجهزة الحاسب الآلي، بوصفه مجرد آلة وانقسمت الآراء إلى اتجاهين:

الاتجاه الأول: وذهب أصحابه إلى أن الحاسب الآلي، ما هو إلا عبارة عن وسيط لهذا التحايل، وأن الطبيعة الإلكترونية لجرائم الحاسب الآلي، لن تضيف أيّ جديد في إطار الاحتيال التقليدي، إلا مجرد الوسيلة المستخدمة، فالاحتيال على الحاسب الآلي للاستيلاء على مال الغير تتحق به الطرق الاحتيالية التقليدية [2]، على اعتبار ما يحدث، ما هو إلا أكاذيب تدعمها مظاهر خارجية، تتمثل بالمعلومات والبيانات، التي تم إدخالها إلى الحاسب الآلي، بحكم أن هنالك دائماً شخص طبيعي يقف وراء النظام الإلكتروني المعلوماتي، الأمر الذي يمكن القول معه، أنّه هو

---

(1) العاني، جرائم الاعتداء على الأموال، ص141.

(2) الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية، ص123.

الشخص ذاته الذي قام بالخداع، بالطرق الاحتيالية التي أتاها الجاني، ويشير جانب من الفقه الفرنسي، والمؤيد لهذا الاتجاه إلى أنّ المشرّع عند صياغته القانون، انحصر وتمركز تفكيره في العلاقات المرتبطة بين البشر فقط، ولم يدر في خلده يوماً أن مثل هذه العلاقات سوف تتطور لتصبح بين البشر والآلة، وأن هذه المسألة، ليست بذات الأهمية بحسب وجهة نظر أصحاب هذا الاتجاه والمؤيدون، فالإنسان هو من يقف وراء الآلة في نهاية الأمر[1].

ويستشهد أصحاب هذا الجانب الفقهي، في تدعيم وجهة نظرهم، بما ذهبت إليه محكمة النقض الفرنسية، بتطبيق عقوبة الاحتيال، على شخص قام بإدخال سيارته إلى مكان انتظار السيارات، وبدلاً من وضع النقود الأصلية المطلوبة، في عداد ماكينة الانتظار، قام بوضع قطع معدنية قديمة عديمة الفائدة، لا تمثل أي قيمة مادية في التعامل، وترتب على ذلك تشغيل الماكينة، وبناءً عليه أسندت المحكمة حكمها على أن وضع القطعة المعدنية عديمة القيمة، في عداد الماكينة، يُعد من قبيل الطرق الاحتيالية، ووفقاً لهذا الاتجاه، فإنّه يمكن تطبيق النصوص التقليدية الخاصة بجريمة الاحتيال، في قانون العقوبات على جرائم الاحتيال الإلكتروني[2].

الاتجاه الثاني: يرى أصحاب هذا الاتجاه، أنّه من غير الممكن القول بصلاحية نظام الحاسب الآلي، لوقوع فعل الاحتيال عليه، وبالتالي عدم اعتباره مجني عليه، لأنّه مجرد آلة، كما أن النصوص التقليدية، التي وضِعتْ في مواجهة جريمة الاحتيال، تفترض أن الطرق الاحتيالية لا بد أن تقع بين أشخاص طبيعيين؛ لأن الإدعاء بالكذب يفترض وجود علاقة مباشرة بين هؤلاء الأشخاص، مما يجعلنا نستدل، بأن الطرق الاحتيالية، نطاقها العلاقات الإنسانية، وليس مجرد آلة من صنع البشر[3]، ووفقاً لهذا الإتجاه فإنّه لابد من استحداث نصوص عقابية تجرم الاحتيال

---

(1) الحفناوي، فاروق على، (2001)، موسوعة قانون الكمبيوتر ونظم المعلومات، الطبعة الأولى، دار الكتاب الحديث للنشر، القاهرة، مصر، ص161.

(2) قورة، جرائم الحاسب الآلي الاقتصادية، ص575.

(3) الشوا، سامي، (1994)، ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الأولى، دار النهضة العربية للنشر، القاهرة، مصر، ص124.

الإلكتروني، بما يتناسب وطبيعة هذه الجرائم المُستحدثة، وهو الاتجاه الذي يتفق معه الباحث؛ لأن محاولة مدّ نصّوص جريمة الاحتيال التقليدية، لتشمل جريمة الاحتيال الإلكتروني تصطدم بمبدأ الشرعية، وإذا نظرنا إلى موقف التشريعات المختلفة، من إمكانية مدى تطبيق الاحتيال، على نظام الحاسب الآلي وإيقاعه بالغلط نكون أمام اتجاهين:

الاتجاه الأول: وفقاً لهذا الاتجاه، فإنّه لا يمكن خداع نظام الحاسب الآلي، بوصفه مجرد آلة، حيث لا بد أن يكون الفاعل، قد خدع إنسان آخر، وبالتالي من غير الممكن تطبيق النص القانوني، الخاص بجريمة الاحتيال التقليدية، على جرائم الاحتيال الإلكتروني، وهذا ما ذهب إليه المشرّع الأردني، في نص المادة (417) من قانون العقوبات عندما استعمل لفظ (الغير)، في مطلع هذه المادة التي نصت على أنه: (كل من حمّل الغير على تسليمه مالاً منقولاً، أو غير منقول، أو اسناداً تتضمن تعهداً أو إبراء فاستولى عليها احتيالاً ...)، وهو نفسه ما ذهب إليه كل من المشرع المصري، واللبناني والإماراتي، والايطالي[1].

الاتجاه الثاني: ويمثل هذا الاتجاه، تشريعات الدول الإنجلوسكسونية، حيث يرجع السبب في إمكانية تطور وقوع الاحتيال، على أجهزة الحاسب الآلي، وإيقاعه بالغلط، بحسب هذه التشريعات، ليس لوجود نصوص صريحة تقضي بذلك، إنما بحكم أن النصوص التشريعية الخاصة، بجرائم الاحتيال التقليدية، تتسم بالعمومية والشمول، ومن الممكن الاستناد على هذه السمات في بعض الأحيان، لتطبيق أحكام تلك النصوص على جرائم الاحتيال الإلكتروني[2].

ثانياً: مدى اعتبار تسليم الأموال البنكية التي يتم التلاعب بها من خلال التحويل الإلكتروني للأموال تسليماً مادياً

النقود البنكية (الإلكترونية): يقصد بها تلك النقود التي يتم تداولها، باستخدام نظم المعالجة الآلية المعلوماتية، وبصفة خاصة، في نظام التحويل الإلكتروني

(1) عفيفي، عفيفي كامل، (2000)، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، الطبعة الأولى، دون ناشر، ص151، 152.

(2) الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، ص125.

للأموال، المعتمد على نظام (Online) وبصورة متكاملة، حيث يتم نقل وتحويل الأموال، من خلال هذا النظام بشكل فوري، في حين تقتضي جريمة الاحتيال التقليدية، أن يقوم الجاني بحيازة المال محل الجريمة حيازة مادية، بحيث يكون الاستيلاء كذلك مادياً من قبل الجاني للمال[1].

ويرى جانب من الفقه أن الاستيلاء الذي يتم عن طريق نظام الحاسب الآلي، لا يرتب أدنى مشكلة، إذا كان محل الاستيلاء نقوداً، كأن يتم التلاعب بالبيانات المدخلة، أو المخرجة في أجهزة الحاسب الآلي، أو برمجته من خلال شخص ما، لكي يستخرج باسمه، أو باسم شركائه شيكات، أو مبالغ مالية غير مستحقة له، ويستولي عليها مادياً[2]، ولكن يُثار التساؤل، في حالة إذا كان محل الاستيلاء في الاحتيال، هو النقود البنكية الالكترونية، أو ما يعرف بالتحويل الإلكتروني للأموال، وهل يعتبر الاستيلاء مادياً، ومحقق لنتيجة جريمة الاحتيال من عدمه؟

نجد جانب من الفقه، يرى أن العِبرة في الاحتيال الإلكتروني، هو قيام الحاسب الآلي بوضع المال محل النشاط الجرمي، تحت يد وتصرف الجاني، من خلال الأساليب الاحتيالية التي مارسها الجاني، وإنّه لا يُشترط أن يتم التسليم أو الاستيلاء بطريقة مادية، أي بالمناولة، وأن التسليم بهذه الحالة لتحويل الأموال، لا يتعارض ومفهوم التسليم في جريمة الاحتيال التقليدية[3].

وهذا ما يميل إليه جانب من الفقه المصري والفرنسي، الأمر الذي أكده القضاء الفرنسي، عندما ابتكرت محكمة النقض الفرنسية، نظرية تسمى (التسليم المعادل) لمواجهة حالات الاحتيال، التي تتم عن طريق التلاعب بضريبة المبيعات، وعداد مواقف السيارات، وعلى الهواتف، لـ يأخذ الفقه بهذه النظرية، لكي يتم بها ملاحقة كل أشكال الاحتيال، باستخدام النظام الإلكتروني والمعلوماتي[4].

---

(1) ذوابه، عقد التحويل الإلكتروني، ص21.

(2) الطوالبة، الجرائم الإلكترونية، ص188.

(3) قورة، جرائم الحاسب الآلي الاقتصادية، ص583.

(4) الرومي، التعاقد الالكتروني عبر الانترنت، ص64.



وبالنسبة لموقف تشريعات بعض الدول، حول هذه المسالة، نجدها على النحو الآتي:

أولاً: ذهبت بعض الدول، إلى الاعتراف بالأموال البنكية، بصفتها أموالاً تصح أن تكون محلاً لجريمة الاحتيال، والسرقة، وخيانة الأمانة، بالرغم من طابعها غير الملموس، مثل تشريعات الولايات المتحدة الأمريكية.

ثانياً: ذهبت دولاً أخرى، إلى عدم اعتبار النقود البنكية، من قبيل الأموال المادية، بل صنفتها ديوناً، ولاً تصلح محل لجريمة الاحتيال، أو السرقة، كما هو الحال في التشريع الألماني والياباني.

ثالثاً: في حين التزمت تشريعات دول أخرى، الصمت حيال هذه المسألة، كما هو حال قانون العقوبات الأردني، وغيره من التشريعات العربية[1].

ثالثاً: اعتبار الوسائل التقنية المستخدمة في جريمة الاحتيال الالكتروني من قبيل الطرق الاحتيالية التي نصت عليها المادة (417) من قانون العقوبات الأردني

كما أسلفت، أن البعض ذهب إلى اعتبار خداع أنظمة الحاسب الآلي، للاستيلاء على مال الغير، تتحقق به الطرق الاحتيالية، مثل الكذب الذي تدعمه أعمال مادية، أو وقائع خارجية، والمتمثلة بالمعلومات والبيانات والبرامج، التي تم إدخالها إلى النظام المعلوماتي، لكي تتم عملية التلاعب[2].

ولكن حتى لو سلمنا، باعتبار أن الوسائل التقنية، المستخدمة في جرائم الاحتيال الإلكتروني، تُعد من قبيل الطرق الاحتيالية، فأن ذلك لا يجعل من تطبيق نص المادة (417) من قانون العقوبات الأردني، على جرائم الاحتيال الالكتروني أمراً ممكناً؛ لأن الطرق الاحتيالية، في الأساس يجب أن تكون في إطار العلاقات الإنسانية، أي بمواجهة إنسان آخر، وليس آلة، وذلك بحسب المفهوم التقليدي لجريمة الاحتيال، وعليه نجد أن المشرّع الأردني، من خلال قانون العقوبات والنصوص المتعلقة بجرائم الاحتيال التقليدية، قد عجزت عن مواكبة تطور تكنولوجيا

---

(1) عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، ص155، 156.
(2) الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، ص127.

المعلومات، التي أدت إلى استحداث عدد من الجرائم، وعلى رأسها جرائم الاحتيال الإلكتروني، وأنّه لابد من وجود قوانين، تنص صراحةً على تجريم هذه الأفعال، أو تعديل النصوص التقليدية، لتشمل في إطارها هذه الجرائم[1].

في حين نجد أن قانون الاتصالات الأردني، رقم (13) لسنة 1995، قد اكتفى بتوفير نوع من الحماية للمعلومات، والبيانات المتبادلة، عبر شبكات الاتصال من خطر الإتلاف، والشطب لمحتويات الرسائل، من خلال نص المادة (76)، والتي تنص على أنّه: (كل من اعترض، أو أعاق، أو صوّر، أو شطب محتويات رسالة بواسطة شبكات الاتصال، أو شجع غيره على القيام بهذا العمل، يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد عن ستة أشهر، أو بغرامة مالية لا تزيد عن (200) مائتي دينار أو بكلتا هاتين العقوبتين)، كما نصت المادة (77) من القانون على أنّ: (كل من أقدم على كتم رسالة، عليه نقلها بواسطة شبكات الاتصال إلى شخص آخر، أو رفض نقل رسائل طُلب منه نقلها من قبل المرخص له، أو الهيئة، أو نسخ، أو أفشى، أو عبث بالبيانات المتعلقة بأحد المشتركين، بما في ذلك أرقام الهواتف غير المعلنة، أو الرسائل المرسلة، أو المستقبلة، يعاقب بالحبس لمدة لا تزيد عن ستة أشهر أو بغرامة لا تزيد عن (1000) ألف دينار أو بكلتا هاتين العقوبتين)[2].

وبحسب رأي الباحث، فإنّه من خلال استعراض هاتين المادتين من هذا القانون، أنّه من غير الممكن تطبيق هذه النصوص، على جرائم الاحتيال الالكتروني، لعدم توافر واكتمال عناصر جريمة الاحتيال الالكتروني، من الركن المادي والركن المعنوي، خصوصاً أن صياغة هذا القانون، جاءت بفترة تعتبر فيها شبكات الاتصال، من أفضل ما أبرزته ثورة تكنولوجيا المعلومات، بحِقبة التسعينيات على الصعيد المحلي الأردني، ولم يكن بالحسبان، تخيل مثل هذه الجرائم، على المدى القريب على أقل تقدير.

ونستدل على عدم إمكانية الأخذ بنصوص هذا القانون، على جرائم الاحتيال الإلكتروني، من خلال تعريف الاحتيال الإلكتروني أنّه: (التلاعب العمدي بمعلومات

---

(1) المومني، الجرائم المعلوماتية، ص206 وما بعدها.

(2) الزعبي والمناعسة، جرائم تقنية نظم المعلومات الإلكترونية، ص254.

وبيانات تمثل قيماً مادية، يختز نها نظام الحاسب الآلي، أو الإدخال غير المصرح به لمعلومات وبيانات صحيحة، أو التلاعب في الأوامر والتعليمات، التي تحكم عملية البرمجة، أو أي وسيلة أخرى، من شأنها التأثير على الحاسب الآلي، حتى يقوم بعملياته بناء على هذه البيانات، أو الأوامر، أو التعليمات من أجل الحصول على ربح غير مشروع، وإلحاق ضرر بالغير)[1].

2.4.2 مدى مواجهة قانون المعاملات الإلكترونية وقانون جرائم أنظمة المعلومات لجرائم الاحتيال الإلكتروني

وعليه سوف نتناول مدى انطباق قانون المعاملات الإلكترونية على جرائم الاحتيال الإلكتروني، ومدى انطباق قانون جرائم أنظمة المعلومات على جرائم الاحتيال الإلكتروني.

أولاً: مدى انطباق قانون المعاملات الإلكترونية على جرائم الاحتيال الإلكتروني

بعد العجز التشريعي لقانون العقوبات الأردني، في التصدي لمثل هذه الجرائم المستحدثة، وما تناوله قانون الاتصالات الأردني، لم يكن بالأداة الرادعة، حيث اقتصرت نصوص هذا القانون بشكل واضح على نظم الاتصالات وما قد يشوبها من تجاوزات، فجاء قانون المعاملات الإلكترونية المؤقت، رقم (85) لسنة 2001 حيثُ تناول عدداً من التعريفات الخاصة بالمصطلحات الإلكترونية، ومشتملاً على (41) مادةحيث جاء في نص المادة (35) على أنّه: (يعاقب كل من يقوم بإنشاء، أو نشر، أو تقديم شهادة توثيق، لغرض احتيالي، أو لأي غرض غير مشروع بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد عن سنتين أو بغرامة لا تقل عن (3000) ثلاثة الآف دينار ولا تزيد عن (10,000) عشرة الآف دينار أو بكلتا هاتين العقوبتين)، وهذه المادة جاءت لتجرم كل الأفعال الاحتيالية، التي تتم بواسطة شهادة التوثيق فقط، ، وبالرجوع إلى نص المادة الثانية، من القانون ذاته نجدها عرفت شهادة التوثيق على أنّهاّ : (الشهادة التي تصدر عن جهة مختصة، مرخصة أو

---

(1) قورة، جرائم الحاسب الآلي الاقتصادية، ص425.

معتمدة، لإثبات نسبة توقيع الكترونـي، إلى شخص معين استناداً إلى إجراءات توثيق معتمدة) وتنص المادة (38) من القانون ذاته على أنّه: (يعاقب كل من يرتكب فعـلاً يشكل جريمة، بموجب التشريعات النافذة، بواسطة استخدام الوسـائل الإلكترونيـة بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سـنة أو بغرامـة لا تقـل عـن (3000) دينار ولا تزيد على (1000) دينار أو بكلتا هـاتين العقـوبتين، ويعاقـب بالعقوبة الأشد إذا كانت العقوبات المقررة في تلك التشريعات، تزيد علـى العقوبـة المقررة في هذا القانون)[1].

وبما أن جرائم الاحتيال الإلكتروني، شأنها شأن أي جريمـة، مـن حيـثُ وجوب توافر الأركان الأساسية للجريمة، فأننا بالنظر إلى وسائل وصور الاحتيـال الإلكتروني، التي يتمثل الركن المادي للجريمة من خلالها، لم نجد ما يجـرم تلـك الأفعال من خلال نص المادتين السابقتين، ولا باقي نصوص القـانون الأخـرى[2]، سواء من خلال التلاعب بالمدخلات، في أجهزة الحاسب الآلي والأنظمة الإلكترونية التي يعمل بها، فالإدخال يُعرّف على أنّه: تزويد الحاسب الآلي والنظام بالبيانـات، والمعلومات المراد معالجتها والتحكم بها آلياً، سواء أكان ذلك التلاعب بحذف هـذه المعلومات أو تغييرها[3]، وهو الأمر ذاته الذي ينطبق علـى التلاعـب بالبيانـات، والمعلومات، بمرحلة الإخراج، والمتمثل بإخفاء المعلومات، أو حـذفها والتلاعـب بالبرامج، وعليه فإنّ هذا القانون لم يـأت بجديـد، ويتـصدى لجـرائم الاحتيـال الإلكتروني، ويسد النقص التشريعي الذي خلفه قانون العقوبات والقوانين الأخرى.

ثانياً: مدى انطباق قانون جرائم أنظمة المعلومات على جرائم الاحتيال الإلكتروني

بعد القصور الذي شاب قانون العقوبات الأردني، وباقي القوانين، في معالجة هذا النوع من الجرائم المستحدثة، فما كان من المشرّع إلا الانتظار حتى منتصف ما

---

(1) الخشروم، عبدالله، (2001)، قانون المعاملات الإلكترونية لعام 2001 وأثره في عمليات البنوك، مؤتمر عمليات البنوك بين النظرية والتطبيق، كلية الحقوق، جامعة اليرموك بالفترة الواقعة بين 22 كانون الأول و24 كانون الأول لسنة 2001، الأردن، ص2، 3.

(2) المومني، الجرائم المعلوماتية، ص207.

(3) قورة، جرائم الحاسب الآلي الاقتصادية، ص432.

بعد العام 2010 وهو تاريخ صدور قانون جرائم أنظمة المعلومات المؤقت، رقم (30)[1]، ومن هنا سنحاول أن نرى، مدى تصدي هذا القانون لجرائم الاحتيال الإلكتروني.

جاء في نص المادة (3) الفقرة (أ) من هذا القانون أنّه : (كل من دخل قصداً موقعاً الكترونياً، أو نظام معلومات بأي وسيلة دون تصريح، أو بما يخالف، أو يجاوز التصريح، يعاقب بالحبس مدة لا تقل عن اسبوع ولا تزيد عن ثلاثة أشهر، أو بغرامة لا تقل عن (100) مائة دينار ولا تزيد عن (200) مائتي دينار أو بكلتا هاتين العقوبتين).

في حين نصت الفقرة (ب) من ذات المادة، على أنّه : (إذا كان الدخول المنصوص عليه في الفقرة (أ) من هذه المادة بهدف إلغاء، أو حذف، أو إضافة، أو تدمير، أو إفشاء، أو إتلاف، أو حجب، أو تعديل، أو تغيير، أو نقل، أو نسخ بيانات، أو معلومات، أو توقيف، أو تعطيل عمل نظام معلومات، أو تغيير موقع الكتروني، أو إلغائه، أو إتلافه، أو تعديل محتوياته، أو إشغاله، أو انتحال صفته، أو انتحال شخصية مالكه فيعاقب الفاعل بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد عن سنة أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد عن (1000) ألف دينار أو بكلتا هاتين العقوبتين).

إنّ المشرّع الأردني، كان أكثر شمولية وتفصيلاً، واستخدم في نصوصه الكثير من المعاني والألفاظ، في محاولة منه لسد النقص التشريعي، عما كان عليه الحال في القوانين السابقة، ومن خلال ما تقدم من شرح لأركان جرائم الاحتيال الإلكتروني سابقاً، من مسار هذا البحث، والمتمثلة بصور ووسائل هذه الجرائم، نرى إمكانية الشرعية بتطبيق نص المادة (3) على عدد من هذه الصور، ومن أهم هذه الصور التلاعب بالمدخلات في أجهزة الحاسب الآلي، وإمكانية تحقيق أركان هذه الجريمة من الركن المادي أي النشاط الذي يقوم به الفاعل بقصد التلاعب بالمدخلات من خلال تغيير البيانات المراد إدخالها، أو بحذفها كلها، أو بحذف جزء منها، أو

---

(1) قانون جرائم أنظمة المعلومات المؤقت رقم (30) لسنة 2010 والمنشور على الصفحة 5334 من عدد الجريدة الرسمية رقم (5056) بتاريخ 2010/9/16.

باستبدالها، أو إتلافها، أو حجبها بصورة غير مشروعة [1]، ونستدل على ذلك أيضاً، إذْ ما قارنا نص المادة (3)، من هذا القانون، بنص المادة (263) الفقرة (أ) من قانون العقوبات الألماني، والتي تنص على أنّه يعتبر مرتكباً لجريمة الاحتيال المعلوماتي: (كل من يقوم بنية تحقيق ربح غير مشروع له، أو لغيره وإلحاق ضرر بالغير، بالتأثير في نتيجة المعالجة الآلية للمعلومات عن طريق برمجة غير سليمة، أو استعمال بيانات غير صحيحة، أو غير مكتملة، أو عن طريق الاستعمال غير المصرح به للبيانات، أو عن طريق التدخل غير المصرح به، في عملية المعالجة الآلية ذاتها)، ومن التشريعات التي تأثرت بنص تلك المادة، نص المادة (386) بالفقرة (أ)، من قانون العقوبات اليوناني، رقم (1805) لسنة 1988 والتي تنص على أنّه: (كل من يقوم بالتأثير في المعلومات المبرمجة، عن طريق برمجة غير سليمة، أو عن طريق التدخل أثناء تطبيق البرامج، أو عن طريق استعمال بيانات غير سليمة، أو غير مكتملة أو بأي طريقة أخرى مما يرتب عليه حدوث إضرار لممتلكات الغير، على أن يكون ذلك بنية إثراء نفسه، أو غيره بربح غير مشروع)[2]، وهنا نكون أمام معالجة حقيقية لأهم صوره من صور الاحتيال الإلكتروني، والتي تعتبر من أكثرها انتشاراً، خصوصاً أنها لا تحتاج إلى مهارات تقنية عاليه من قبل مرتكبها، وتطبق هذه المادة على هذا النوع من الجرائم، التي تقع ممن يُصرح لهم الدخول لهذه البيانات، مثل موظفي البنوك والشركات المالية، وغيرهم وممن لا يحق لهم الدخول[3].

وهذا ما أكدته الفقرة (أ) من نص المادة (3)، من القانون الأردني، ونجد أن هذا التصدي للتلاعب بالبيانات والمعلومات، في مرحلة الإدخال، لا يختلف عنه من حيث النشاط المجرّم للفاعل، والقصدية والغاية عنه، في صورة التلاعب بالبيانات والمعلومات، في مرحلة الإخراج، والمسماة (Out put manipulation)

---

(1) المومني، الجرائم المعلوماتية، ص196.

(2) قورة، جرائم الحاسب الآلي الاقتصادية، ص599.

(3) المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية، ص333.

والمتمثلة في التلاعب بالبيانات والمعلومات، في مرحلة إخراج هذه البيانـــات مـــن خلال تعديلها، أو إلغائها، أو حجبها، أو حذفها كلها، أو جزء منه،ا من أجل تحقيـــق الغاية الاحتيالية لهذا الفاعل[1].

ومن وسائل وأساليب الاحتيال الإلكتروني، والتي من الممكن أن نجد مـــن نصوص هذا القانون مـــا يعالجهـــا، ألا وهـــي التلاعـــب بـــالبرامج (Programs Manipulation) وإنْ كانت من الحالات الأقل حـــدوثاً، وتحتـــاج إلـــى اشـــخاص متخصصين، في التعامل مع البرامج الإلكترونية، حيث تتمثل هذه الـــصورة، مـــن خلال التلاعب بالبرامج بإلغاء، أو حذف جزء من البيانات، أو اســـتبدالها ببـــرامج أخرى، ليتمكن الفاعل من القيام بجرمه الاحتيالي، سواء أكان هذا النشاط المجـــرّم، وقع من قبل أشخاص مصرح لهم الدخول، أم ممن لا يحق لهم الدخول، إلـــى هـــذه الأنظمة المعلوماتية[2].

وجاء التصدي لهذه الحالة، واضح وصريح، من خلال نص المادة (4) من ذات القانون، والّتِي تنص على أنّه : (كل من دخل، أو نـــشر، أو اســـتخدم قـــصداً برنامجاً عن طريق الشبكة المعلوماتية، أو باستخدام نظام معلومات، بهدف إلغاء أو حذف أو إضافة، أو تدمير، أو إفشاء، أو إتلاف، أو حجب، أو تعديل، أو تغيير، أو نقل، أو نسخ، أو التقاط، أو تمكين الآخرين من الاطلاع على بيانات، أو معلومات، أو إعاقة، أو تشويش، أو إيقاف، أو تعطيل عمل نظام معلومات، أو الوصول إليـــه، أو تغيير موقع الإلكتروني، أو إلغائه، أو إتلافه، أو تعديل محتوياته، أو إشـــغاله، أو انتحال صفته، أو شخصية مالكه دون تصريح، أو بما يجـــاوز التـــصريح يعاقـــب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد عن سنة أو بغرامة لا تقل عن (200) مائتي دينار ولا تزيد عن (1000) ألف دينار أو بكلتا هاتين العقوبتين).

ونلاحظ أن نص المادة الرابعة، قد ساوى بالعقوبة المقررة، في نص المادة الثالثة، من ذات القانون، وحاول أن يرفد نـــص المـــادة الرابعـــة، بـــالكثير مـــن المصطلحات والمعاني التي تم الإشارة، إليها بنص المادة الثالثة، في محاولـــة منـــه

(1) قورة، جرائم الحاسب الآلي الاقتصادية، ص444.

(2) حماد، جرائم الحاسوب، ص32 وما بعدها.

لتجريم الكثير من الأفعال، من دون أن يقتصر ذلك على مادة دون الأخرى، ويمكن أن نستدل أيضاً على حجية ما سبق بإمكانية تطبيق النصوص السابقة، على صور الاحتيال الإلكتروني، التي ذكرت من خلال التعريف الذي صدر عن هيئة الأمم المتحدة، والخاص بالاحتيال الإلكتروني على أنّه ": (إدخال لبيانات، أو محوها، أو تعديلها، أو كبتها، أو برامج حاسوب، أو التدخل المؤثر في معالجة البيانات، التي تسبب خسارة اقتصادية، أو فقد حيازة ملكية شخص، أو آخر بقصد الحصول على كسب اقتصادي، غير مشروع له، أو لشخص آخر)[1].

أما فيما يتعلق بالأفعال المجرمة، التي تمارس من خلال الاستخدام غير المشروع، لبطاقات الدفع الإلكتروني، نجد أن قانون جرائم أنظمة المعلومات، قد اغفل بعض من هذه الأفعال، ولم يجرمها، مثل استصدار بطاقات الائتمان بمستندات مزورة، التي يقدمها طالب البطاقة للبنك المصدر، وإساءة استخدام البطاقة بعد انتهاء صلاحيتها، وغيرها من صور التلاعب بالبطاقات[2]، في حين تناول القانون، الاعتداء الذي يتم على بيانات هذه البطاقات، والاستيلاء عليها من خلال الشبكة المعلوماتية، أو الأنظمة التي تخزن عليها بيانات ومعلومات البطاقات، من خلال نص المادة (6) الفقرة (أ) والتي تنص على أنّه ": (كل من حصل قصداً دون سبب مشروع، عن طريق الشبكة المعلوماتية، أو أي نظام معلومات على بيانات، أو معلومات بطاقات الائتمان، أو البيانات أو المعلومات التي تستخدم في تنفيذ المعاملات المالية، أو المصرفية الإلكترونية، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد عن سنتين أو بغرامة لا تقل عن (500) خمسمائة دينار ولا تزيد عن (2000) ألفي دينار أو بكلتا هاتين العقوبتين)، في حين نصت الفقرة (ب) من ذات المادة على أنّه ": (كل من استخدم عن طريق الشبكة المعلوماتية، أو أيّ نظام معلومات قصداً دون سبب مشروع بيانات، أو معلومات بطاقات الائتمان، أو البيانات أو المعلومات التي تستخدم في تنفيذ المعاملات المالية، أو المصرفية الإلكترونية للحصول لنفسه، أو لغيره على بيانات أو معلومات، أو أموال أو خدمات

---

(1) المومني، الجرائم المعلوماتية، ص189.

(2) زين الدين، جرائم نظم المعالجة الآلية للبيانات، ص145 وما بعدها.

تخص الآخرين، يُعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن (1000) ألف دينار ولا تزيد عن (5000)خمسة آلاف دينار)، إن نص هذه المادة، قد جاء واضح وصريح، في تجريم العديد من صور وأشكال جرائم الاحتيال الإلكتروني، بواسطة بطاقات الدفع الإلكتروني ومن أهم هذه الصور:

أولاً: الاعتداء على نظام بطاقة الائتمان، من خلال التاجر، عند استخدام البطاقة من قبل حاملها، من خلال جهاز نقاط البيع (p.o.s)، عندما يقوم التاجر بتمرير البطاقة أكثر من مرة؛ بغية الحصول على أكثر من إشعار، ليسارع بتعبئته ومطالبة البنك بقيمة هذا الإشعار[1]، وأجهزة نقاط البيع، تُعتبر نظام معلوماتي، كما نصت المادة، بعبارة أي نظام معلوماتي.

ثانياً: الاعتداء على نظام بطاقة الائتمان، من قبل موظفي البنك، حيث يَشرع موظف البنك، باستغلال وظيفته، بالاستيلاء على بيانات البطاقات، من أجل استخدامها للحصول على أموال الغير، سواء من خلال التواطؤ مع العميل نفسه، أو الغير، أو التاجر[2]، وهذا ما أكدته الفقرة (ب) من ذات المادة، من خلال قصدية الاستيلاء، غير المشروع على هذه البيانات، من أجل تنفيذ معاملات مالية.

ثالثاً: الاعتداء على بيانات بطاقات الائتمان، من خلال شبكة الانترنت، وهي الحالة التي يستطيع من خلالها حامل البطاقة، الشراء والتسوق من خلال شبكة الانترنت، التي توفر عليه عناء الذهاب للأسواق والمتاجر، أو في حالة عدم توفر بعض السلع، في الأسواق المحلية، وهو ما يُسمى بالتجارة الإلكترونية، حيث يُخدع الكثير ممن يحملون البطاقات ، بتزويد بياناتهم لشركات تقدم السلع، يتبين فيما بعد، أنّها شركات وهمية لا أساس لوجودها، أو من خلال الدفع بتحويل الأموال، بواسطة البطاقة، من قبل حاملها، لأصحاب هذه المواقع الاحتيالية[3]، وهو ما نصت عليه المادة (6) الفقرة (ب)، من خلال ذكر استخدام الشبكة المعلوماتية، وهو معنى واسع

(1) القضماني، البطاقة المصرفية والانترنت، ص125.

(2) مصطفى، جرائم الحاسبات الآلية في التشريع المصري، ص301.

(3) أبو شامة، عولمة الجريمة الاقتصادية، ص90.



يشمل العديد من الأفعال غير المشروعة، التي يُهدف من ورائها الاستيلاء على أموال الغير.

رابعاً: الاحتيال الإلكتروني من خلال أنظمة الحوالات البنكية الإلكترونية:

ومن الممكن أن نستدل على ذلك، من خلال التحويل الإلكتروني للأموال، والذي عُرّفعلى أنّه : عملية تبادل ونقل الأموال، بصورة الكترونية، بدلاً من الوسائل الكتابية التقليدية [(1)]، وهو ما ينطبق على التجريم الذي تناولته المادة السابقة، الفقرة (ب)، من خلال تنفيذ المعاملات المصرفية الإلكترونية، لنفسه أو لغيره، على بيانات أو معلومات أو أموال، تخص الآخرين بصورة غير مشروعة.

ومن جهة نظر الباحث، إنّ ما تطرقت إليه المادة (6) من هذا القانون، وتجريم الأفعال عن طريق بطاقات الدفع الإلكتروني، لم تكون بالشكل الوافي، وأنّه كان على المشرع الأردني، إنْ يحذو ما سارت علية الكثير من التشريعات العربية، بتخصيص نصوص قانونية، خاصة لمواجهة جرائم البطاقات الإلكترونية، بشكل أكثر تفصيلاً، كما فعل التشريع القطري، الذي تناول كل ما يتعلق ببطاقات الدفع الإلكتروني، مثل تقليدها أو تواطئ موظف البنك، في تسريب أرقام البطاقات، أو تصنيع البطاقات بصورة غير مشروعة، والتي لم يعالج الـ مشرع الأردني الكثير، منها حيث أقتصر في معالجته لجرائم بطاقات الدفع الإلكتروني فقط، في نص المادة (6) الفقرة (أ) و (ب) من قانون جرائم أنظمة المعلومات، خصوصاً أن الانتشار الذي باتت عليه بطاقات الدفع الإلكتروني، أصبحت من عصب الحياة الاقتصادية والاجتماعية، لتسهيل عملية تبادل ونقل الأموال، أيّ أن الأمر لم يعد حكراً على

---

(1) السرحان والمشهداني، أمن الحاسوب والمعلومات، ص112. تنص المادة (383) من قانون العقوبات القطري على أنّه: (يعاقب بالحبس مدة لا تقل عن سنة ولا تجاوز خمسة سنوات، وبالغرامة التي لا تقل عن عشرة آلاف ريال، ولا تزيد على عشرين ألف ريال كل من:

أ. زور بطاقة دفع آلي.

ب. استعمل بطاقة دفع آلي مزورة، أو مسروقة مع علمه بذلك.

ج. قبل بطاقات دفع آلي غير سارية، أو مزورة، أو مسروقة، مع علمه بذلك.

د. صنع المعدات، أو الآلات المستخدمة في صناعة بطاقات الدفع الآلي بدون ترخيص.



التعاملات البنكية فقط، وهذا ما تحدثنا عنه في قسم سابق، من خلال المواجهة التشريعية، لجرائم بطاقات الدفع الإلكتروني.

ونختم بنص المادة (13) الفقرة (أ)، التي تناولت دور الجهات الأمنية (الضابطة العدلية)، بكيفية التعامل في تطبيق نصوص هذا القانون، حيث نصت المادة على أنّه : (مع مراعاة الشروط والأحكام المقررة، في التشريعات ذات العلاقة، يجوز لموظفي الضابطة العدلية، الدخول إلى أيّ مكان يشتبه باستخدامه، لارتكاب أيّ من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة، والأدوات، والبرامج والأنظمة، والوسائل المشتبه في استخدامها، لارتكاب أيّ من تلك الجرائم، باستثناء بيوت السكن، إلا بإذن من المدعي العام المختص قبل الدخول إليها، وفي جميع الأحوال على الموظف الذي قام بالتفتيش، أن ينظم محضراً بذلك، ويقدمه إلى المدعي العام المختص).

3.4.2 دور الأجهزة الأمنية والجهات المتخصصة في الحد من جرائم الاحتيال الإلكتروني في الأردن

بات من الواجب النظر، إلى مثل هذا النوع من الجرائم، بشيء من الجدية، والبحث عن الحل المناسب، بعد أن بينا مخاطر هذه الجرائم، ومن أوائل الحلول، وسبل الوقاية وجوب التعاون بين كل من الدوائر الرسمية، وباقي الأجهزة المرتبطة، بتقنيات الإعلام والاتصال المحلي، والدولي، من أجل إنشاء الهيئات والأقسام الخاصة، في مكافحة جرائم الاحتيال الإلكتروني[1].

ومن جهة نظر الباحث، أن كل ما يرافق حركات التقدم والازدهار، والثورة المعلوماتية، أصبح ينتشر في الكيان المجتمعي بصورة سريعة، على عكس ما كان عليه الوضع سابقاً، وذلك نتيجة الاستخدام المباشر، والسريع لتكنولوجيا المعلومات، وأن نقطة ولادة الخطر، تتمركز في آلية التعامل المفرط والعشوائي اللاواعي في كيفية إدراك مخاطر كل ما هو جديد، وأن جُل النظر، ينصب على الجانب المشرق

---

(1) سفر، أنظمة الدفع الإلكتروني، ص22.

فقط من هذه الخدمات الإلكترونية فهنالك من ينغمس بها من خلال سعيه لتطوير البحث العلمي، والتقدم الصناعي، ومنهم من يتخذ منها أداة ترفيهية، ومنهم من جعل الغاية من استخدامها أداةً للتفاخر وهكذا..

في حين تم إغفال الجانب الآخر، من هذه الدوامة العصرية، والتي اتخذ منها البعض أسلوب عيش وكسب غير مشروع، وطوّعها لتكن أداةٌ تُهدد المجتمع على الصعيد المحلي والدولي، وأن جرائم الاحتيال الإلكتروني، لم تعد كما كانت في بداياتها، محدودة النطاق على مستوى الدول المتقدمة، بل أصبحت في نطاق أوسع، ومهما حاولت التشريعات، والأجهزة المتخصصة، الحدّ من ارتكاب هذا النوع من الجرائم فإنها لن تستطيع أن تسير معها بنفس السرعة المطلوبة؛ لما يتطلبه التشريع من إجراءات طويلة، وعليه يقع على عاتق المجتمع، وبكل فئاته أن يكون هو المبادر، للحدّ من ارتكاب هذا النوع من الجرائم؛ لما له من مساس مباشر، بأمن وحماية الأفراد، وتتمثل هذه المبادرة من خلال التوعية لمثل هذه المخاطر، ابتداءً من الأسرة، مروراً بالمراحل الدراسية المتوسطة، وصولاً إلى المراحل التعليمية المتقدمة، مثل الجامعات، لكي يتسنى لإفراد المجتمع، من تلقي أساليب التوعية والإرشاد، بشكل أكثر فعالية وتشاركيه، والتعاون أيضاً، من قبل الجهات المختصة، وإدارة الإعلام بكافة فروعه المختلفة، وبهذه الحالة لا يقع كل العبء على كاهل المشرع، والأجهزة الأمنية ذات الاختصاص وحدها، فنحن لا نبحث عن مجتمع نقي بالكامل، بل إلى الحد الأدنى من نسب ارتكاب أيّ جريمة، وعلى رأسها جرائم الاحتيال الإلكتروني، والتي سُرعان ما تتطور لتصبح ظاهرة إجرامية، تحتاج إلى جهدٍ كبير من أجل مكافحتها والحدّ من انتشارها.

وفي الأردن، نجد هنالك جهداً كبير للحد من جرائم الاحتيال الإلكتروني، والجرائم الإلكترونية بشكل عام، مقارنةً بدول العالم الثالث وإمكانياتها، فقد قامت إدارة البحث الجنائي، التابعة لمديرة الأمن العام، بإنشاء قسم خاص يسمى : (قسم جرائم تكنولوجيا المعلومات والإسناد الفني)، حيثُ يستطيع أيّ شخص تعرض لعملية احتيالية، أو اشتبه بأي عمل احتيالي أن يلجأ إلى إدارة البحث الجنائي، والتي بدورها توصل المشتكي إلى المختصين بهذا القسم، والذي يرتبط مع الكثير من

الدول الإقليمية والدولية في بروتوكولات ونشاطات للتعاون في الحد من تفاقم هــذه الظاهرة الإجرامية[1]، ومن الواجبات التي تلقى على عاتق قسم تكنولوجيا المعلومات والإسناد الفني:

1. التحقيق بجرائم تكنولوجيا المعلومات والاتصالات وجرائم الانترنت.
2. تقديم الخبرة الفنية الميدانية، والدعم الفني في مسرح الجريمــة فــي جــرائم الاحتيال المالي، والجرائم الأخرى ذات العلاقة.
3. تقديم الدعم الفني لعمليات المراقبة، والتعقب الفني، والاتصال.

أما على صعيد التوعية الشعبية، فإن القسم ينصح باتبــاع الأفــراد بعــض الإجراءات الوقائية على النحو التالي:

1. عدم السماح للغرباء باستخدام جهاز الحاسوب الخاص بهم.
2. استخدام كلمة مرور معقدة للملفات والمستندات والبريد الإلكتروني.
3. عدم إعطاء اسم المــستخدم (username) أو كلمــة المــرور (password) لأي شخص.
4. تجديد وتغيير كلمات المرور بشكل دوري كل شهرين على سبيل المثال.
5. عدم إعطاء المعلومات الشخصية لأي جهة غير موثوق بهــا عبــر البريــد الإلكتروني[2].

أما على صعيد الأسرة فينصح القسم باتباع ما يلي:

1. مراقبة استخدام الأبناء لأجهزة الحاسوب، وطبيعة المواقع التــي يتــصفحونها بشكل مستمر وحثيث.
2. ملاحظة أيّ تصرفات قد تظهر بسلوك الأبناء، ومواجهتهم بالتحدث الايجــابي بعيداً عن التعنيف لتجنب تفاقم الأمور.
3. عدم التردد في طلب المساعدة الأمنية إذا تطلب الأمر.

أما على صعيد الشركات والمؤسسات فينصح بما يلي:

---

(1) الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية، ص282.

(2) الموقع الإلكتروني الآتي: http://www.cdd.psd.gov.jo/index.php?option=com_content&task=view&id=263&Itemid=300 p.1&2,of 3,date7/9/2011

1. التحديث المستمر لمواقع الشركات، والمؤسسات باستخدام احدث البرامج، ومواكبتها بشكل مستمر.
2. تغيير كلمة المرور بشكل دوري للموظفين.
3. تغيير اسم المستخدم وكلمة المرور، لأي موظف يستقيل من عمله، أو تم إيقافه، واستلامه منه بشكل رسمي.
4. تجنب استخدام كلمات المرور الدارجة والمتوقعة، مثل اسم أحد الأبناء، أو رقم الهاتف، أو تاريخ الميلاد وهكذا...
5. مراجعة البنك في حال ورود بريد الكتروني، يدّعي أنّه موجه من هذا البنك لتأكد من صحة هذا البريد.
6. عدم التردد بالاتصال بالجهات الأمنية المتخصصة، في حال وجود أي شُبهات للاحتيال الإلكتروني.

علماً أنّ هذا القسم المختص، يتعهد بمعالجة هذه القضايا بسرية تامة بينه وبين من يلجأ إليه من المشتكين والمتضررين[1].

5.2 الخاتمة

أن التسارع الملحوظ لتكنولوجيا المعلومات، بات يخلق فضاءً واسعاً ومرتعاً لجرائم الاحتيال الإلكتروني، والذي لابد أن يقابله تسارعٌ، منٌ قبل المشرّع بسن القوانين، التي تواجه هذه الجرائم، وتكثيف التعاون بين الجهات المتخصصة من أجل الوصول إلى الآلية المناسبة للحدّ من هذه الجرائم على الصعيد المحلي، والاستفادة من الخبرات الدولية الأخرى في هذا المجال.

وقد تناولنا في هذه الدراسة، توضيح مفهوم جرائم الاحتيال الإلكتروني، ووسائله وأدواته وبعض أنماط هذه الجرائم، بالإضافة إلى معرفة موقِف التشريعات المقارنة من هذه الجريمة، وقد توصل الباحث إلى مجموعة من النتائج والتوصيات، نوردها على النحو الآتي:

---

(1) مقابله أجراها الباحث: مع رئيس قسم جرائم تكنولوجيا المعلومات والإسناد الفني في دائرة البحث الجنائي، مديرية الأمن العام بتاريخ 2010/11/18.



أولاً: النتائج

1النقص التشريعي المعالج لجرائم الاحتيال الإلكتر وني، في كل من قانون العقوبات الأردني، وقانون المعاملات الإلكترونية، وقانون الاتصالات الأردني مقارنةً مع غيره من التشريعات العربية والأجنبية.

2. صدور قانون جرائم أنظمة المعلومات الأردني المؤقت، رقم 30 لسنة 2010 والذي تناول عدداً من جرائم الاحتيال الإلكتروني، و أن كان لم يتمتع بالشمولية لتصدي الكامل لهذا النوع من الجرائم.

3. دور الأجهزة الأمنية الفاعلة على الصعيد المحلي في مكافحة هذا النوع من الجرائم من خلال الجهود التي يبذلها قسم جرائم تكنولوجيا المعلومات والإسناد الفني في دائرة البحث الجنائي، مديرة الأمن العام، الأردن.

4. عدم إمكانية تطبيق النصوص الخاصة بجريمة الاحتيال التقليدية بحسب نص المادة (417) من قانون العقوبات الأردني على الأفعال الاحتيالية لجرائم الاحتيال الإلكتروني.

5. خلو قانون جرائم أنظمة المعلومات من أي نص يجرم الشروع في جرائم الاحتيال الإلكتروني أسوةً بباقي التشريعات التي جرمت الشروع بهذه الجرائم.

6. الاهتمام التشريعي بجرائم الاحتيال الإلكتروني، في الكثير من الدول الأجنبية والمتقدمة من أوائل عقد الثمانينات، وهو ما سارت علية العديد من تشريعات دول الخليج العربي مثل التشريع القطري، والتشريع السعودي.

7.عدم وجود اتفا ق أو نص تشريعي يبين مفهوم جرائم الاحتيال الإلكتروني، لتفاوت انتشار تكنولوجيا المعلومات ومخاطرها، من بلد إلى آخر، وحداثة هذه الجرائم.

8. إنّ جُل مرتكزات وأدوات واساليب جرائم الاحتيال الإلكتروني، مرتبطة بالاستخدام غير المشروع، المبني على الحيلة والخداع، لتكنولو جيا المعلومات وهذا ما يميزها، عن جرائم الاحتيال بمفهومها التقليدي.

9. إنّ جرائم الاحتيال الإلكتروني تُعتبر من الجرائم العابرة للحدود، على اعتبار أن وسائل الاتصال المتطورة، المرتبطة بتكنولوجيا المعلومات وشبكة الانترنت، تُعد البيئة والأدوات المكونةِ، لارتكاب هذا النوع من الجرائم.
10. إنّ جرائم الاحتيال الإلكتروني، قد تطال الكثير من حقوق الإفراد، بشتى المجالات، وإن كانت البنوك، والمؤسسات المالية، والشركات ذات النصيب الأوفر بالاستهداف في هذا النوع من الجرائم.
11. إنّ من أشهر جرائم الاحتيال الإلكتروني، تلك المتعلقة بالاحتيال، من خلال أجهزة الحاسب الآلي والتلاعب بها، والاستخدام غير المشروع، لبطاقات الدفع الإلكتروني، والتحويل غير المشروع للأموال، بقصد الاستيلاء عليها، ورسائل البريد الإلكتروني الخادعة عبر شبكة الانترنت.
12. إن أنجع وسائل مكافحة جرائم الاحتيال الإلكتروني بالمقام الأول، هو بث التوعية الإرشادية، والتحذيرية اللازمة، من أجل تجنب الوقوع بهذا الشرك الاحتيالي.
13. أن الدافع الأساسي في ارتكاب مثل هذه الجرائم الإثراء، أو حب الظهور.

ثانياً: التوصيات

1. العمل على إعادة النظر في النصوص التشريعية، المتعلقة بتكنولوجيا المعلومات، بإفراد نصوص أكثر تخصص، لجرائم الاحتيال الإلكتروني على الصعيد المحلي.
2. سد النقص التشريعي المتعلق بالنصوص المجرّمة، للاستخدام غير المشروع لبطاقات الدفع الإلكتروني، بشكل أكثر تفصيلاً، أسوةً ببعض التشريعات الأجنبية والعربية، كالتشريع الفرنسي، والايطالي، والقطري.
3. تعديل نص المادة (6) من قانون جرائم أنظمة المعلومات المؤقت رقم (30) لسنة 2010 التي تضمنت فقرتين بإضافة فقرة ثالثة (ج) تنص على أنّه (كل من قلد بطاقة دفع الإلكتروني، أو قبل التعامل ببطاقات مقلدة، أو مسروقة، أو منتهية الصلاحية، أو صنّع الآلات المستخدمة في صناعة بطاقات الدفع الإلكتروني، أو ساهم بذلك بطريقة غير مشروعة، وبدون ترخيص، عوقب



بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن (1000) ألـــف دينـــار ولا تزيد عن (5000) خمسة آلاف دينار).

4. إضافة نص يعاقب على الشروع في قانون جرائم أنظمة المعلومات الأردني على النحو الآتي : (يعاقب كل من شرع فـــي القيـــام بـــأي مـــن الجـــرائم المنصوص عليها في هذا القانون بما لا يتجاوز نصف الحد الأعلى للعقوبـــة المقررة).
5. إضافة نص إلى القانون ذاته يخفف أو يعفي من العقوبة للجنـــاة فـــي حـــال عدولهم عن الجريمة على النحو الآتي : (للمحكمة المختـــصة أن تعفـــي، أو تخفف من هذه ا لعقوبات، لكل من يبادر من الجناة بإبلاغ السلطات المختصة بالجريمة، قبل علم السلطات بها، وقبل وقوع الضرر، إذ كان من شأن هـــذا الإبلاغ ضبط باقي الجناة، أو الأدوات المستخدمة في ارتكاب الجريمة).
6. تكثيف التعاون بين الجهات الأمنية المختصة، بمكافحـــة هـــذا النـــوع مـــن الجرائم، مع السلطة التشريعية، لمواكبة تطور هذه الجرائم، ووضع الآليـــة المناسبة، للحد من جرائم الاحتيال الإلكتروني.
7. تفعيل دور الإعلام بكافة وسائله؛ للمساهمة في بث التوعية الإرشادية، لتصل إلى أكبر شريحة ممكنة من الأفراد، كون جرائم الاحتيال الإلكتروني، تـــدق معظم الأوساط المجتمعية.
8. تفعيل دور مؤسسات المجتمـــع المحلـــي، والجمعيـــات، والمنتـــديات ذات الاختصاص، في المساهمة في بث التوعية، بين أفراد المجتمع ككل، حـــول هذا النوع من الجرائم.
9. عقد الدورات الإرشادية اللازمة، لتعريّف بجرائم الاحتيال الإلكتروني، بشكل أكثر فاعلية، للعاملين في القطاعين العام والخاص، ســـيما قطـــاع البنـــوك، والشركات المالية والاستثمارية.
10. دعم الدراسات الخاصة بتطوير الأمن المعلوماتي، لتضييق على مرتكبـــي الجرائم الإلكترونية بشكل عام، ومرتكبي جرائم الاحتيال الإلكتروني بـــشكل



خاص، لأن من شأن ذلك توفير الثقـــة اللازمـــة، بالمعـــاملات، والتجـــارة الإلكترونية.

المراجع

أ. المراجع العربية:

إبراهيم، خالد ممدوح، (2011)، **حوكمة الانترنت**، الطبعة الأولى، دار الفكر الجامعي للنشر، الإسكندرية، مصر.

أبو الروس، أحمد بسيوني، (1986)، **جرائم النصب**، دار المطبوعات الجامعية للنشر، الإسكندرية، مصر.

أبو جريش، جورج؛ ورشوان، خشان يوسف، (2004)، **المدخل إلى مصارف الانترنت**، الطبعة الأولى، إتحاد المصارف العربية للنشر، بيروت، لبنان.

أبو خطوة، أ حمد، (1990)**الجرائم الواقعة على الأموال** ، الطبعة الأولى، دار البيان للنشر، دبي، الإمارات.

أبو شامة، عباس، (2008)، **عولمة الجريمة الاقتصادية**، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية.

أحمد، عبد الرحمن توفيق، (2005)، **الجرائم التي تقع على الأموال في قانون العقوبات الأردني**، الطبعة الأولى، دار وائل للنشر، عمان، الأردن.

أحمد، مؤمن، (2005)**أمن الانترنت المخاطر والتحديات**، مكتب نائب رئيس مجلس الوزراء لشؤون الإعلام، أبو ظبي، الإمارات.

آل عدينان، عبدالله محمد، (2011)، **الاحتيال المعلوماتي**، مركز التميز لأمن المعلومات، متوفر عبر الموقع: www.coeia.edu.sa.

البحر، ممدوح خليل، (2008)، **الجرائم الواقعة على الأموال في قانون العقوبات الإماراتي**، الطبعة الأولى، دار أثراء للنشر، عمان، الأردن.

البطراوي، عبدالوهاب، (2007)**شرح جرائم ضد الأموال** ، الطبعة الأولى، جامعة العلوم التطبيقية، البحرين.

البغدادي، كميت طالب، (2008)، **الاستخدام غير المشروع لبطاقة الائتمان**، الطبعة الأولى، دار الثقافة للنشر، عمان، الأردن.



بهنام، رمسيس، (1982)، **القسم الخاص في قانون العقوبات** ، دار المعارف للنشر، الإسكندرية، مصر.

التحالف العالمي لمكافحة التصيد الاحتيالي متوفر عبر الرابط: www.antiphishing.org.

إدارة البحث الجنائي، **قسم جرائم تكنولوجيا المعلومات والإسناد الفني** ، مديرية الأمن العام، الأردن.

توفيق، عبدالرحمن؛ ونجم، محمد صبحي، (1983)، **شرح قانون العقوبات الأردني**، الجزء الأول، الطبعة الأولى، دار التوفيق للنشر، عمان، الأردن.

الجبور، محمد، (1997)، **الجرائم الواقعة على الأموال** ، الطبعة الأولى، دار الثقافة للنشر، عمان، الأردن.

جعفر، علي محمد، (2006)، **قانون العقوبات القسم الخاص** ، الطبعة الأولى، دار مجد للنشر، بيروت، لبنان.

الجهني، أمجد حمدان، (2010)، **المسؤولية المدنية عن الاستخدام غير المشروع لبطاقات الدفع الإلكتروني**، الطبعة الأولى، دار المسيرة للنشر، عمان ، الأردن.

الجيوشي، طاهر خليل، (2001)، **جرائم الاحتيال الأساليب والوقاية والمكافحة** ، الطبعة الأولى، أكاديمية نايف للعلوم الأمنية، الرياض، السعودية.

حافظ، مجدي محب، (2000)، **جرائم النصب والاحتيال والجرائم الملحقة بها**، دار الكتب القانونية للنشر، الإسكندرية، مصر.

حجازي، عبدالفتاح بيومي، (2009)، **علم الجريمة والمجرم المعلوماتي**، الطبعة الأولى، دار المعارف للنشر، الإسكندرية، مصر.

الحفناوي، فاروق علي، (2001)، **موسوعة قانون الكمبيوتر ونظم المعلومات**، الطبعة الأولى، دار الكتاب الحديث للنشر، القاهرة، مصر.

حماد، محمد، (2006)، **جرائم الحاسوب**، الطبعة الأولى، دار المناهج للنشر، عمان، الأردن.

الحيط،عادل عزام سقف ، (2011)، **جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية**، الطبعة الأولى، دار الثقافة للنشر، عمان، الأردن.

الخشروم، عبدالله، (2001)، **قانون المعاملات الإلكترونية لعام 2001وأثره في عمليات البنوك**، مؤتمر عمليات البنوك بين النظرية والتطبيق ، كلية الحقوق، جامعة اليرموك بالفترة الواقعة بين 22 كانون الأول و 24كانون الأول ، الأردن.

الدبيان، دبيان محمد، (2011)، بطاقات الائتمان والتكييف الفقهي، متوفر عبر الموقع: www.alukah.net.

ذوابة، محمد عمر، (2006)، **عقد التحويل الإلكتروني**، الطبعة الأولى، دار الثقافة للنشر، عمان، الأردن.

رباح، غسان، (2008)، **الوجيز في قضايا الملكية الفكرية والفنية مقارنة مع الجريمة المعلوماتية**،الطبعة الأولى، م شورات الحلبي الحقوقية، بيروت، لبنان.

الربيعي، حيدر غازي، (2008)، جريمة الاحتيال في مجال التجارة الإلكترونية، **مجلة القادسية للقانون والعلوم السياسية**، العدد الثالث، ص 11.

الرومي، محمد أمين، (2004)،**التعاقد الالكتروني عبر الانترنت** ، الطبعة الأولى، دار المطبوعات الجامعية للنشر، الإسكندرية، مصر.

الزعبي، جلال محمد؛ والمناعسة، أسامة أحمد، (2010)، **جرائم تقنية نظم المعلومات الإلكترونية**، الطبعة الأولى، دار الثقافة للنشر، عمان، الأردن.

زين الدين، بلال، (2008)، **جرائم نظم المعالجة الآلية للبيانات**، الطبعة الأولى، دار الفكر الجامعي للنشر، الإسكندرية، مصر.

السرحان،سرحان سليمان ؛ والمشهداني، محمود، (2001)، **أمن الحاسوب والمعلومات**، دار وائل للنشر، عمان، الأردن.

سفر، أحمد، (2008)، **أنظمة الدفع الإلكتروني**، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان.

السقا، إيهاب فوزي، (2007)، **الحماية الجنائية والأمنية لبطاقات الائتمان** ، الطبعة الأولى، دار الجامعة الجديدة للنشر، الإسكندرية، مصر.

سلامة، عماد، (2005)، **الحماية القانونية لبرامج الحاسب الآلي ومشكلة قرصنة البرامج**، الطبعة الأولى، دار وائل للنشر، عمان، لبنان.

الشاذلي،فتوح عبد الله ، (1996)، **جرائم الاعتداء على الأشخاص والأموال**، دار المطبوعات الجامعية للنشر، الإسكندرية، مصر.

الشناوي، محمد، (2007)، **جرائم النصب المستحدثة** ، دار شتات للنشر، القاهرة، مصر.

الشوا، سامي، (1994)، **ثورة المعلومات وانعكاساتها على قانون العقوبات** ، الطبعة الأولى، دار النهضة العربية للنشر، القاهرة، مصر.

الشوابكة، محمد أمين، (2004)، **جرائم الحاسوب والانترنت (الجريمة المعلوماتية)**، الطبعة الأولى، دار الثقافة للنشر، عمان، الأردن.

الشورة، جلال عايد، (2008)، **وسائل الدفع الإلكتروني** ، الطبعة الأولى، دار الثقافة للنشر، عمان، الأردن.

الشيخني، عبدالقادر، (2009)، **جريمة الاحتيال**، الطبعة الأولى، منشورات الحلبي، بيروت، لبنان.

صالح، نائل عبدالرحمن، (1996)، **الوجيز في الجرائم الواقعة على الأموال** ، الطبعة الأولى، دار الفكر الجامعي للنشر، عمان، الأردن.

صالح، نائل عبدالرحمن، (1996)، **شرح قانون العقوبات القسم الخاص الجرائم الواقعة على الأموال**، دار الفكر الجامعي للنشر، عمان، الأردن.

الطوالبة، علي حسن، (2008)، **الجرائم الإلكترونية**، الطبعة الأولى، جامعة العلوم التطبيقية، البحرين.

عاطف، زياد، (د.ت)، **الاحتيال الإلكتروني من مشكلة إلى أزمة** ، متوفر عبر الموقع: www.coeia.edu.sa.

العاني، عادل إبراهيم، (1995)، **جرائم الاعتداء على الأموال** ، الطبعة الأولى ، دار الثقافة للنشر، عمان، الأردن.

عبابنة، محمود، (2004)**جرائم الحاسوب وأبعادها الدولية**، دار الثقافة للنشر، عمان، الأردن.

عبد الحليم، عماد الدين، (2010)، **المعاملات المصرفية بواسطة الهواتف النقالة**، رسالة ماجستير غير منشورة، كلية الحقوق، جامعة الشرق الأوسط، عمان، الأردن.

عبد الغني، سمير، (2007)**جرائم الاعتداء على الأموال**، دار شتات للنشر، القاهرة، مصر.

عبدالرحيم،وجدي عصام ، (2011)**سرقة البطاقات الائتمانية من أجهزة الصراف الآلي**، متوفر عبر الموقع: www.coeia.edu.sa.

العبدان،روان عبدالرحمن ، (2011)**تطبيقات آمنه في عمليات الدفع الإلكتروني** ، متوفر عبر الموقع: www.coeia.edu.sa.

العبودي، عباس، (2010)، **تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني**، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان.

عرب، يونس، (2002)، **جرائم الكمبيوتر والانترنت** ، مؤتمر الأمن العربي للدراسات والبحوث الجنائية، أبوظبي بالفترة الواقعة من 10 إلى 2002/2/12.

العريان، محمد علي، (2004)، **الجرائم المعلوماتية**، دار الجامعة الجديدة للنشر، الإسكندرية، مصر.

العريفي،جوهرة بنت عبدالعزيز ، (2011)،**الخداع داخل الانترنت** ، مركز التميز لأمن المعلومات، متوفر عبر الموقع: www.coeia.edu.sa.

العسبلي، منى شاكر، (د.ت)**تأثير الجريمة الإلكترونية على النواحي الاقتصادية**، متوفر عبر الموقع: www.coeia.edu.sa.

عفيفي، عفيفي كامل، (2000)**جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية**، الطبعة الأولى، دون ناشر.

الغثبر،خالد بن سليمان ؛ والقحطاني محمد بن عبدالله، (2008)، **الاصطياد الإلكتروني**، الطبعة الأولى، جامعة الملك سعود، الرياض، السعودية.



الغثبر، خالد بن سليمان؛ والقحطاني،محمد بن عبدالله ، (2009)، **أمن المعلومات** ، الطبعة الأولى، جامعة الملك سعود، الرياض، السعودية.

غنام، شريف محمد، (2007)**محفظة النقود الإلكترونية رؤية مستقبلية** ، الطبعة الأولى، دار الجامعة الجديدة للنشر، الإسكندرية، مصر.

الفوزان،صالح بن محمد ، (2011)**البطاقة الائتمانية تعريفها وأخذ الرسوم على إصدارها والسحب النقدي بها**، متوفر عبر الموقع: www.saaid.net/fatwa.

فوزي، نجاح محمد، (2007)، **وعي المواطن العربي تجاه جرائم الاحتيال"بطاقات الدفع الإلكتروني نموذجا**،جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية.

الفيل، علي عدنان، (2011)، **الإجرام الإلكتروني**، الطبعة الأولى، منشورات زين الحقوقية، بيروت، لبنان.

قانون الأمارات العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها متوفر عبر الرابط :
http://arabic.mjustice.dz/liguearabe/loi_emir_ar_crim_tech_info.pdf

قانون جرائم أنظمة المعلومات المؤقت رقم (30) ، 2010، **الجريدة الرسمية** ص 5334، عدد 5056، بتاريخ 2010/9/16.

قانون العقوبات القطري، (2004)، رقم (11)، متوفر عبر الرابط:
www.gcc_legal.org/mojportalpublic/BrowseLawOption.aspx?country=3&LawID=2597

قانون تكنولوجيا المعلومات الهندي (المعدل)، 2008، متوفر عبر الرابط:
http://www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf

القضماني، حسين إبراهيم، (2002)، **البطاقة المصرفية والانترنت**، الطبعة الأولى، اتحاد المصارف العربية للنشر، بيروت، لبنان.

قورة، نائله، (2005)**جرائم الحاسب الآلي الاقتصادية** ، الطبعة الأولى، منشورات الحلبي الحقوقية، القاهرة، مصر.

كريدلي، نهاد، (2011)**الجريمة والاحتيال في البيئة الإلكترونية** ، متوفر عبر الموقع: http://www.nasbcom.net/vb/showthread.php

المجالي، نظام توفيق، (2005)**شرح قانون العقوبات القسم العام** ، الطبعة الأولى، دار الثقافة للنشر، عمان، الأردن.

محمد، شيماء عبدالغني، (2007)، **الحماية الجنائية للتعاملات الإلكترونية**، الطبعة الأولى، دار الجامعة الجديدة للنشر، الإسكندرية، مصر.

محمد، عوض، (1987)،**جرائم الأشخاص والأموال** ، دار المطبوعات الجامعية، الإسكندرية، مصر.

محمد، مصطفى، (2011)**دور الانتربول الدولي بمكافحة الجريمة** ، متوفر عبر الموقع: www.qanon302.net/news/news.php?action=view&id=5998

المحمدي، حسنين، (2008)، **إرهاب الانترنت الخطر القادم**، الطبعة الأولى، دار الفكر الجامعي للنشر، الإسكندرية، مصر.

المدني، سليمان، (1995)،**الاحتيال علم وفن** ، الطبعة الأولى، دار المنارة للنشر، بيروت، لبنان.

مراد، عبد الفتاح، (1996)، **شرح جرائم النصب وخيانة الأمانة والجرائم الملحقة بها**، الطبعة الأولى، دار الفتح للنشر، القاهرة، مصر.

مصطفى، أحمد، (2010)**جرائم الحاسبات الآلية في التشريع المصر** ي، الطبعة الأولى، دار النهضة للنشر، الإسكندرية، مصر.

المطيري، أنور بدر، (د.ت)**ظاهرة جرائم الكمبيوتر والانترنت** ، متوفر عبر الموقع: www.lawweb.cc/d1/d7.doc

المكاوي، محمد محمود، (2010)،**الجوانب الأخلاقية والاجتما عية والمهنية للحماية من الجرائم المعلوماتية** ، الطبعة الأولى، المكتبة العصرية للنشر، القاهرة، مصر.

المكتبي، زاد، (2007)**تكنولوجيا المعلومات وتطبيقاتها في حياتنا** ،جريدة القدس ، متوفر عبر الموقع: www.arablibrariannet.blogspot.com.



الملط، أحمد خليفة، (2001)، **الجرائم المعلوماتية**، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، مصر.

المنشاوي، عبدالحميد، (1990)، **جرائم النصب والاحتيال في ضوء القضاء والفقه**، دار الفكر الجامعي، الإسكندرية، مصر.

منشاوي، محمد عبدالله، (2011)، **جرائم الانترنت من منظور شرعي وقانوني**، متوفر عبر الموقع: http://www.dahsha.com/old/viewarticle

منصور، محمد حسين، (2003)، **المسؤولية الإلكترونية**، دار الجامعة الجديدة للنشر، الإسكندرية، مصر.

المومني، نهلا عبدالقادر، (2007)، **الجرائم المعلوماتية**، الطبعة الأولى، دار الثقافة للنشر، عمان، الأردن.

نبيه، نسرين عبدالحميد، (2008)، **الجريمة المعلوماتية والمجرم المعلوماتي**، دار المعارف للنشر، الإسكندرية، مصر.

نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية رقم (79) لسنة 2007 متوفر عبر الرابط:
http://www.ala7ebah.com/upload/showthread.php?69359

نمور، محمد سعيد، (2007)، **شرح قانون العقوبات الجرائم الواقعة على الأموال**، الطبعة الأولى، دار الثقافة للنشر، عمان، الأردن.

هرجة، مصطفى مجدي، (2004)، **جرائم النصب وخيانة الأمانة والجرائم المرتبطة**، دار محمود للنشر، الإسكندرية، مصر.

هرول، نبيله، (2007)، **الجوانب الإجرائية لجرائم الانترنت**، الطبعة الأولى، دار الفكر الجامعي للنشر،الإسكندرية، مصر.

يوسف، أمير فرج، (2008)، **الجرائم المعلوماتية على شبكة الانترنت**، الطبعة الأولى، دار المطبوعات الجامعية للنشر، الإسكندرية، مصر.

ب. المراجع الأجنبية:

Graycar, A. & Smith, R., (2002), **Identifying and Responding to Electronic Fraud Risks**, 30th Australasian Registrars Conference Canberra.



Internet Fraud Complaint Center (IFCC), (2001), **Six-Month Data Trends Report**, National White Collar Crime Center and the Federal Bureau of Investigation.

Jarret, M. & Bailie, M., (2008), **Prosecuting Computer Crimes**, office of legal Education Executive office for United states Attorneys.

Johnson, A., (2010), Stand up for banking at ABA,s GR Summit. **ABA banking journal**. Vol. 2 p 1&2.

Kunz, M. & Wilson, p., (2004), **"Computer Crime and fraud",** Report to the Montgomery County Criminal Justice Coordinating Commission.

Ryan, p. & Harbison, A., (2010), **The Law on computer Fraud in Lreland**, development of law and dishonesty, Grant Thorton.

Sauter, D., (1998), Electronic fraud on campus. **The electronic campus.** Vol6. p96.

Shipley, T. & Hutchings, C., (2010), **Report on Cyber Crime investigation**, A Report of the International High Tech Crime investigation Association.

Singleton, T., (2010), Guard Against Gybertheft. **Journal of Accountancy**. Vol5, p56.

المعلومات الشخصية

الاسم : حمزه عاطف علي المعايطة

الكلية : الحقوق

التخصص : قانون جنائي

السنه : 2012

الهاتف النقال: 0797505668

البريد الالكتروني : hamzeh.atef@gmail.com